Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide, Release 1.6.x

First Published: 2016-05-25

Last Modified: 2018-01-08

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

Preface vii

Audience vii

Document Conventions vii

Related Documentation ix

Obtaining Documentation and Submitting a Service Request xi

CHAPTER 1

New and Changed Information 1

New and Changed Information 1

CHAPTER 2

Overview 3

About the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) 3

Cisco APIC-EM Components and Architecture 6

Appliances 6

Hosts 6

Grapevine 7

Root and Clients 7

Services 7

Databases 7

Networks 7

Network Connections and NICs 8

CHAPTER 3

Troubleshooting Matrix 9

Troubleshooting Matrix 9

CHAPTER 4

Troubleshooting an Installation or Update 15

Troubleshooting the Installation 15

Confirming Network Access to the Controller 17

Confirming that Core Services are Running 18
Updating Cisco APIC-EM Using the Apply Update Script 19
Updating Cisco APIC-EM Using the Apply Update Script (Releases 1.0.2.8, 1.0.3.4) 21

CHAPTER 5 Troubleshooting the Configuration 23
Troubleshooting the Configuration 23
Updating the Configuration Using the Wizard 24
Resetting the Cisco APIC-EM 25
Restoring the Controller to the Factory Default 27
Creating a Support File for a Single Host 29

CHAPTER 6 Troubleshooting Cisco APIC-EM Single and Multi-Host 31
Recovery Procedures for Cisco APIC-EM Node Failures 31
Removing a Single Host from a Multi-Host Cluster 36
Removing a Faulted Host from a Multi-Host Cluster 37
Resetting the Cisco APIC-EM 39
Adding a New Host to a Multi-Host Cluster 41
Shutting Down and Starting Up a Host in a Multi-Host Cluster 45
Confirming the Multi-Host Cluster Configuration Values 47
Changing the Settings in a Multi-Host Cluster 49

CHAPTER 7 Troubleshooting Services Using System Health 51
About Cisco APIC-EM Services 51
Service Managers and Monitors 51
Service Features 52
Services 52
Reviewing the Service Version and Status Using the SYSTEM HEALTH Tab 53
Removing a Service Instance Using the SYSTEM HEALTH Tab 55
Creating a Service Instance Using the SYSTEM HEALTH Tab 56

CHAPTER 8 Troubleshooting Services Using the Controller Admin Console 59
About Cisco APIC-EM Services 59
Service Managers and Monitors 59
Service Features 60
Services 60

Controller Admin Console 61

Reviewing the Service's Version, Status, and Logs 62

Removing a Service Instance 64

Creating a Service Instance 66

CHAPTER 9 Troubleshooting Using the Logs 69

Viewing Audit Logs 69

Changing the Logging Level 71

CHAPTER 10 Troubleshooting Passwords 73

Performing Password Recovery with an Existing Administrator 73

Performing Password Recovery with No Existing Administrator 73

Performing Password Recovery for the Linux Grapevine User Account 74

CHAPTER 11 Troubleshooting Commands 77

Root Commands 77

Client Commands 81

CHAPTER 12 Troubleshooting Log Files 83

Root Log Files 83

Client Log Files 84

CHAPTER 13 Contacting the Cisco Technical Assistance Center 87

Contacting the Cisco Technical Assistance Center 87

Preface

- Audience, page vii
- Document Conventions, page vii
- Related Documentation, page ix
- Obtaining Documentation and Submitting a Service Request, page xi

Audience

This publication is for experienced network administrators who will deploy the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) in their network. Use this guide to troubleshoot any issues with the Cisco APIC-EM.

For additional information about installation for the Cisco APIC-EM, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide* .

For information about using the controller's GUI for the first time, see the *Cisco APIC-EM Quick Start Guide*.

Note The Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) is also referred to within this upgrade guide as a controller.

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in **bold** font.

Convention	Description
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`Courier` font	Terminal sessions and information the system displays appear in `courier` font.
`Bold Courier` font	**`Bold Courier`** font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x | y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document may use the following conventions for reader alerts:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem.*

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time.* You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Documentation

This section lists the Cisco APIC-EM and related documents available on Cisco.com at the following url:

http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-series-home.html

- Cisco APIC-EM Documentation:
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes*
  - *Cisco APIC-EM Quick Start Guide* (directly accessible from the controller's GUI)
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*
  - *Open Source Used In Cisco APIC-EM*
- Cisco EasyQoS Application for Cisco APIC-EM
  - *Cisco EasyQoS Application for APIC-EM Release Notes*
  - *Cisco EasyQoS Application for APIC-EM Supported Platforms*
  - *Cisco EasyQoS Application for APIC-EM User Guide*
- Cisco Network Visibility Application for the Cisco APIC-EM
  - *Cisco Network Visibility Application for APIC-EM Release Notes*
  - *Cisco Network Visibility Application for APIC-EM Supported Platforms*

- *Cisco Network Visibility Application for APIC-EM User Guide*

- Cisco Path Trace Application for Cisco APIC-EM
  - *Cisco Path Trace Application for APIC-EM Release Notes*
  - *Cisco Path Trace Application for APIC-EM Supported Platforms*
  - *Cisco Path Trace Application for APIC-EM User Guide*

- Cisco IWAN Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco IWAN*
  - *Release Notes for Cisco Intelligent Wide Area Network Application (Cisco IWAN App)*
  - *Configuration Guide for Cisco IWAN on Cisco APIC-EM*
  - *Software Configuration Guide for Cisco IWAN on APIC-EM*
  - *Open Source Used in Cisco IWAN and Cisco Network Plug and Play*

- Cisco Network Plug and Play Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco Network Plug and Play*
  - *Solution Guide for Cisco Network Plug and Play*
  - *Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*
  - *Cisco Network Plug and Play Agent Configuration Guide* or *Cisco Open Plug-n-Play Agent Configuration Guide* (depending on the Cisco IOS XE release)
  - *Mobile Application User Guide for Cisco Network Plug and Play*

- Cisco Active Advisor Documentation for the Cisco APIC-EM:
  - *Cisco Active Advisor for APIC-EM Release Notes*

- Cisco Integrity Verification Documentation for the Cisco APIC-EM:
  - *Cisco Integrity Verification Application (Beta) for APIC-EM Release Notes*
  - *Cisco Integrity Verification Application (Beta) for APIC-EM User Guide*

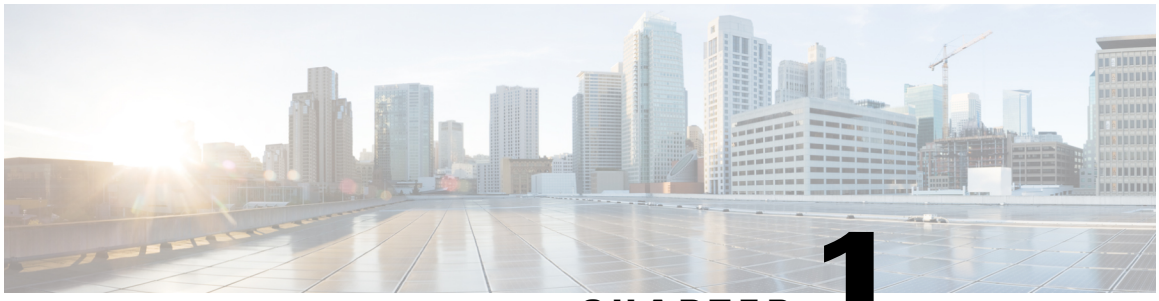
- Cisco Remote Troubleshooter Documentation for the Cisco APIC-EM:
  - *Cisco Remote Troubleshooter Application for APIC-EM Release Notes*
  - *Cisco Remote Troubleshooter Application for APIC-EM User Guide*

Note For information about developing your own application that interacts with the controller by means of the northbound REST API, see the https://developer.cisco.com/site/apic-em/ Web site.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.



CHAPTER 1

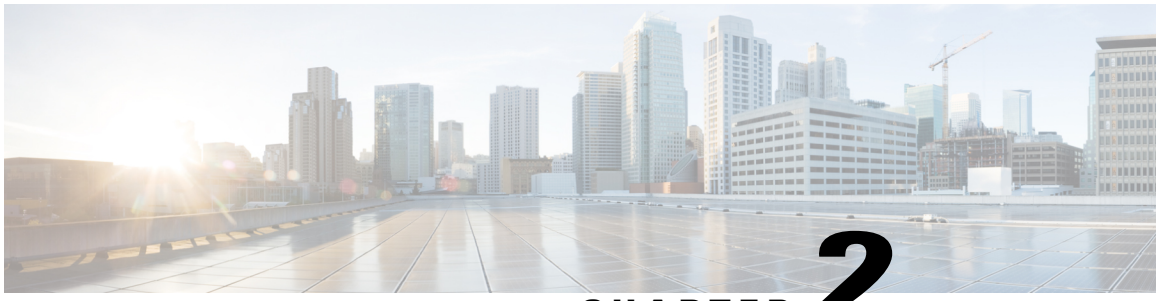
New and Changed Information

- New and Changed Information, page 1

New and Changed Information

There is no new and/or changed information in this guide from its previous release.

New and Changed Information



CHAPTER 2

Overview

- About the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), page 3
- Cisco APIC-EM Components and Architecture, page 6

About the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM)

The Cisco Application Policy Infrastructure Controller - Enterprise Module (APIC-EM) is Cisco's Software Defined Networking (SDN) Controller for Enterprise Networks (Access, Campus, WAN and Wireless).

The platform hosts multiple applications (SDN apps) that use open northbound REST APIs that drive core network automation solutions. The platform also supports a number of south-bound protocols that enable it to communicate with the breadth of network devices that customers already have in place, and extend SDN benefits to both greenfield and brownfield environments.

The Cisco APIC-EM platform supports both wired and wireless enterprise networks across the Campus, Branch and WAN infrastructures. It offers the following benefits:

- Creates an intelligent, open, programmable network with open APIs
- Saves time, resources, and costs through advanced automation
- Transforms business intent policies into a dynamic network configuration
- Provides a single point for network wide automation and control

The following table describes the features and benefits of the Cisco APIC-EM.

Table 1: Cisco APIC Enterprise Module Features and Benefits

Feature	Description
Network Information Database	The Cisco APIC-EM periodically scans the network to create a “single source of truth” for IT. This inventory includes all network devices, along with an abstraction for the entire enterprise network.

Feature	Description
Network topology visualization	The Cisco APIC-EM automatically discovers and maps network devices to a physical topology with detailed device-level data. The topology of devices and links can also be presented on a geographical map. You can use this interactive feature to troubleshoot your network.
EasyQoS application	The EasyQoS application abstracts away the complexity of deploying Quality of Service across a heterogeneous network. It presents users with a workflow that allows them to think of QoS in terms of business intent policies that are then translated by Cisco APIC-EM into a device centric configuration.
Cisco Network Plug and Play (PnP) application	The Cisco Network PnP solution extends across Cisco's enterprise portfolio. It provides a highly secure, scalable, seamless, and unified zero-touch deployment experience for customers across Cisco routers, switches and wireless access points. **Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*.
Cisco Intelligent WAN (IWAN) application	The separately licensed IWAN application for APIC-EM simplifies the provisioning of IWAN network profiles with simple business policies. The IWAN application defines business-level preferences by application or groups of applications in terms of the preferred path for hybrid WAN links. Doing so improves the application experience over any connection and saves telecom costs by leveraging cheaper WAN links. **Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*.
Cisco Active Advisor application	The Cisco Active Advisor application for APIC-EM offers personalized life cycle management for your network devices by keeping you up-to-date on: • End-of-life milestones for hardware and software • Product advisories, including Product Security Incident Response Team (PSIRT) bulletins and field notices • Warranty and service contract status **Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*.

Feature	Description
Cisco Integrity Verification application	The Cisco Integrity Verification (IV) application provides automated and continuous monitoring of network devices, noting any unexpected or invalid results that may indicate compromise. The objective of the Cisco IV application is early detection of the compromise, so as to reduce its impact. The Cisco IV application operates within the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) as a beta version for this release. **Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*.
Cisco Remote Troubleshooter application	The Cisco Remote Troubleshooter application uses the Cisco IronPort infrastructure to create a tunnel that enables a support engineer to connect to an APIC-EM cluster and troubleshoot issues with your system. The app uses outbound SSH to create a secure connection to the cluster through this tunnel. As an administrator, you can use the Remote Troubleshooter application to control when a support engineer has access to a particular cluster and for how long (since a support engineer cannot establish a secure tunnel on their own). You will receive indication that a support engineer establishes a remote access session, and you can end a session at any time by disabling the tunnel they are using.
Public Key Infrastructure (PKI) server	The Cisco APIC-EM provides an integrated PKI service that acts as Certificate Authority (CA) or sub-CA to automate X.509 SSL certificate lifecycle management. Applications, such as IWAN and PnP, use the capabilities of the embedded PKI service for automatic SSL certificate management.
Path Trace application	The path trace application helps to solve network problems by automating the inspection and interrogation of the flow taken by a business application in the network.
High Availability (HA)	HA is provided in N+ 1 redundancy mode with full data persistence for HA and Scale. All the nodes work in Active-Active mode for optimal performance and load sharing.
Back Up and Restore	The Cisco APIC-EM supports complete back up and restore of the entire database from the controller GUI.
Audit Logs	The audit log captures user and network activity for the Cisco APIC-EM applications.

Cisco APIC-EM Components and Architecture

The Cisco APIC-EM consists of the components and architecture discussed in this section. To better troubleshoot any issues with the Cisco APIC-EM, you should review the topics in this section.

Appliances

The Cisco APIC-EM can be deployed on either a physical or virtual appliance.

- For physical appliance support, the Cisco APIC-EM can be installed on the following Cisco UCS servers:
  - Cisco APIC-EM has been tested and qualified to run on these servers.
    - Cisco UCS C220 M4S Server
    - Cisco UCS C220 M3S Server
    - Cisco UCS C22 M3S Server
  - Any Cisco UCS server that meets the minimum system requirements as listed in the *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*.
  - A physical appliance can also be a *dedicated* Cisco UCS server. The following two physical appliances are currently available:
    - Cisco APIC-EM Controller Appliance 10C-64G-2T (APIC-EM-APL-R-K9)
    - Cisco APIC-EM Controller Appliance 20C-128G-4T (APIC-EM-APL-G-K9)

Note Contact Cisco support for additional information about the above appliances and for ordering information.

- For virtual appliance support, the Cisco APIC-EM can also be installed and deployed in a virtual machine that meets the minimum system requirements on VMware vSphere. For information about these requirements, see the *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*

Hosts

A host is defined as an appliance, physical server, or virtual machine running instances of the Grapevine clients. The Grapevine root itself runs directly on the host's operating system. You can set up either a single-host or multi-host deployment. A multi-host deployment with three hosts is best practice for both high availability and scale. Each Grapevine root in a multi-host configuration maintains an Active/Active status with the other Grapevine roots and is therefore able to coordinate with the other Grapevine roots the overall management of the cluster.

Note For additional information about a multi-host deployment, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Grapevine

The Cisco APIC-EM creates a Platform as a Service (PaaS) environment for your network, using Grapevine as an Elastic Services platform to support the controller's infrastructure and services. The Grapevine root and clients are key components of this infrastructure.

Root and Clients

The Grapevine root handles all policy management in regards to service updates, as well as the service life cycle for both itself and the Grapevine client. The Grapevine client is where the supported services run.

For a list of the supported services for this release, see the About Cisco APIC-EM Services, on page 51.

Note You can remotely log into the root using SSH (Secure Shell) to troubleshoot any issues. A default idle timeout of 1 hour has been set for an SSH console login. You will be automatically logged out after 1 hour of inactivity on the SSH console.

Services

The Cisco APIC-EM creates a Platform as a Service (PaaS) environment for your network. A service in this PaaS environment is a horizontally scalable application that adds instances of itself when demand increases, and frees instances of itself when demand decreases.

For a list of the supported services for this release, see the About Cisco APIC-EM Services, on page 51.

Databases

The Cisco APIC-EM supports two databases: application and Grapevine. The application database is used for the application and external networking data. The Grapevine database is used for the Grapevine and internal network data. Both databases are replicated in a multi-host environment for scale and high availability.

Networks

The Cisco APIC-EM architecture requires both external and internal networks to operate:

- The external network(s) consists of the network hosts, devices, and NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI.

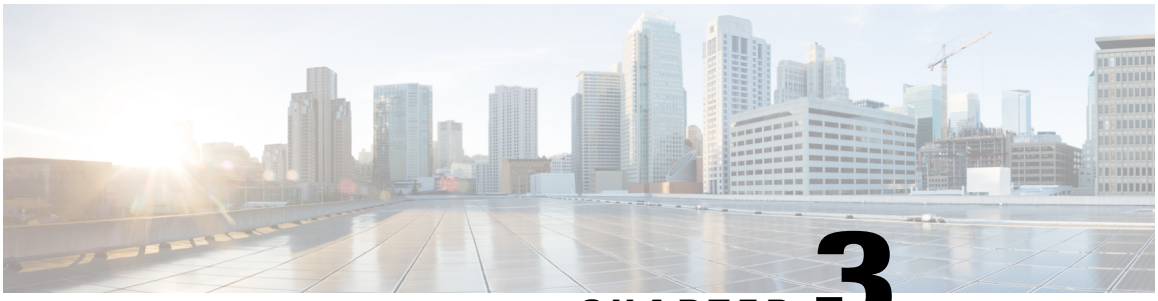
- The internal network consists of the Grapevine roots and clients that are connected to and communicate with each other (service to service). For forwarding to or receiving traffic from the larger external network (that consists of the connected devices and hosts, as well as NTP servers), all inbound and outbound traffic for this internal network passes through a subset of clients connected to the external network. The internal network is isolated and nonroutable from the external network(s), as well as any other internal network.

Network Connections and NICs

The network adapters (NICs) on the host (physical or virtual) are connected to the following external networks:

- Internet (network access required for **Make A Wish** requests, Telemetry, and trustpool updates)
- Network with NTP server(s)
- Network with devices that are to be managed by the Cisco APIC-EM

Note The Cisco APIC-EM should never be directly connected to the Internet. It should not be deployed outside of a NAT configured or protected datacenter environment.



CHAPTER 3

Troubleshooting Matrix

- Troubleshooting Matrix, page 9

Troubleshooting Matrix

The following table lists solutions for the most common issues that relate to Cisco APIC-EM. Reference is made to the relevant chapters and topics throughout this guide.

Table 2: Cisco APIC-EM Troubleshooting Matrix

Symptom	Possible Cause	Recommended Action
Installation Issues		
Failed or unsuccessful installation on a bare-metal server.	Attempted installation of the controller is being made without meeting the system requirements for the release.	Access the latest Cisco APIC-EM release notes and review the system requirements. Be sure to review the appropriate specific system requirements for a bare-metal installation.

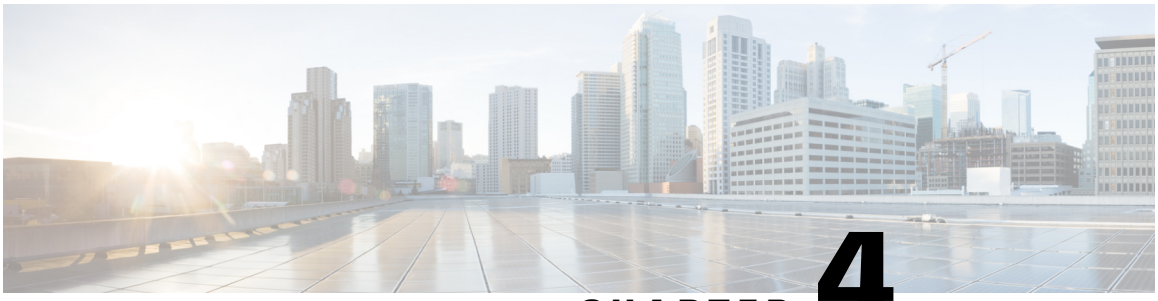
Symptom	Possible Cause	Recommended Action
Failed or unsuccessful installation on a virtual machine.	Attempted installation of the controller is being made without meeting the system requirements for the release.	Access the latest Cisco APIC-EM release notes and review the system requirements. Be sure to review the appropriate specific system requirements for a virtual machine installation, including the VMware resource pool requirements. **Note** For additional assistance with deploying the controller in a virtual machine, refer to the appendix in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide* that discusses virtual machine preparation.
Failed or unsuccessful installation on either a bare-metal server or virtual machine.	Core services failing to start up on the Cisco APIC-EM.	Perform the following actions: • If possible, log into the controller's GUI. • Review the state of the controller services in the **Systems Health** tab. • Create an rca file and send to support for additional assistance. References: • Reviewing the Service Version and Status Using the SYSTEM HEALTH Tab, on page 53 • Creating a Support File for a Single Host , on page 29
Unable to log into the controller GUI after an apparently successful installation.	Network connectivity to the controller is failing.	Review and test your network connections to the controller. Reference: • Confirming Network Access to the Controller, on page 17

Symptom	Possible Cause	Recommended Action
Update Issues		
Unable to update Cisco APIC-EM using the recommended standard methods.		Run the *apply_update* script. Reference: • Updating Cisco APIC-EM Using the Apply Update Script, on page 19
Configuration Issues		
Controller in a *single-host* configuration appears to be in an unstable state. For example, applications are not running, are inaccessible, and/or not appearing in the GUI.	Controller in unstable state, possibly due to error(s) in entering configuration values with the Cisco APIC-EM configuration wizard.	Log into the host, check the configuration values, and reenter any configuration values that are incorrect. References: • Updating the Configuration Using the Wizard, on page 24
Controller in a *multi-host* configuration appears to be in an unstable state. For example, applications are not running, are inaccessible, and/or not appearing in the GUI.	Controller in unstable state, possibly due to error(s) in entering configuration values with the Cisco APIC-EM configuration wizard.	Log into the host, check the configuration values, and reenter any configuration values that are incorrect. References: • Changing the Settings in a Multi-Host Cluster, on page 49
Controller was working fine for a period of time after its initial deployment, but then lapses into an unstable state. For example, applications are not running, are inaccessible, and/or not appearing in the GUI.	Possible user or other error in configuration values that occurs after the initial deployment.	Revert back to the first configuration or the factory default configuration. References: • Resetting the Cisco APIC-EM, on page 25 • Restoring the Controller to the Factory Default, on page 27

Symptom	Possible Cause	Recommended Action
Controller was working fine for a multi-host configuration, but after a period of time one of the hosts becomes erratic and unstable.	Possible failed service or services in the multi-host cluster.	Remove and then reattach unstable host from the multi-host cluster. References: • Removing a Single Host from a Multi-Host Cluster , on page 36
Controller was working fine for a multi-host configuration, but after a period of time one of the hosts *fails*.	Possible failed service or services in the multi-host cluster.	Remove and then reattach failed and inoperable host from the multi-host cluster. References: • Removing a Faulted Host from a Multi-Host Cluster, on page 37
Hardware Issues		
Single host (on an physical appliance or server) reboots, but the controller is not returning to former status.	Services are failing as a result of the reboot and not restarting	If possible, log into the controller's GUI, determine the failed service, restart the service. **Note** You can review the status of controller services using the controller's GUI. References: • Reviewing the Service Version and Status Using the SYSTEM HEALTH Tab, on page 53 • Removing a Service Instance Using the SYSTEM HEALTH Tab, on page 55 • Creating a Service Instance Using the SYSTEM HEALTH Tab, on page 56
Service Issues		

Symptom	Possible Cause	Recommended Action
Service failure on a host that leads to one or more applications on the controller failing. For example, getting a "503 Service Unavailable" message when trying to access the Controller UI.		If possible, log into the controller's GUI, determine the failed service, restart the service. **Note** You can review the status of controller services using the controller's GUI. References: • Reviewing the Service Version and Status Using the SYSTEM HEALTH Tab, on page 53 • Removing a Service Instance Using the SYSTEM HEALTH Tab, on page 55 • Creating a Service Instance Using the SYSTEM HEALTH Tab, on page 56
Password Issues		
Lost password for controller access.	A user (administrator, installer or observer) has lost their password, and there exists at least one controller administrator (ROLE_ADMIN) user account.	Perform the appropriate password recovery for this scenario. References: • Performing Password Recovery with an Existing Administrator, on page 73
Lost password for controller access.	A user (administrator, installer or observer) has lost their password and there exists only one controller administrator (ROLE_ADMIN) user account and that account cannot be successfully logged into.	Perform the appropriate password recovery for this scenario. References: • Performing Password Recovery with No Existing Administrator, on page 73
Lost password for system access.	The Linux grapevine user password has been lost.	Perform the appropriate password recovery for this scenario. References: • Performing Password Recovery for the Linux Grapevine User Account, on page 74

Troubleshooting Matrix



CHAPTER 4

Troubleshooting an Installation or Update

The following information may be used to troubleshoot an unsuccessful installation or update:

- Troubleshooting the Installation, page 15
- Confirming Network Access to the Controller, page 17
- Confirming that Core Services are Running, page 18
- Updating Cisco APIC-EM Using the Apply Update Script, page 19

Troubleshooting the Installation

The following table describes recommended actions to take to resolve a Cisco APIC-EM installation or update issue.

Symptom	Possible Cause	Recommended Action
Failed or unsuccessful installation on a bare-metal server.	Attempted installation of the controller is being made without meeting the system requirements for the release.	Access the latest Cisco APIC-EM release notes and review the system requirements. Be sure to review the appropriate specific system requirements for a bare-metal installation.

Symptom	Possible Cause	Recommended Action
Failed or unsuccessful installation on a virtual machine.	Attempted installation of the controller is being made without meeting the system requirements for the release.	Access the latest Cisco APIC-EM release notes and review the system requirements. Be sure to review the appropriate specific system requirements for a virtual machine installation, including the VMware resource pool requirements. **Note** For additional assistance with deploying the controller in a virtual machine, refer to the appendix in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide* that discusses virtual machine preparation.
Failed or unsuccessful installation on either a bare-metal server or virtual machine.	Core services failing to start up on the Cisco APIC-EM.	Perform the following actions: • If possible, log into the controller's GUI. • Review the state of the controller services in the **Systems Health** tab. • Create an rca file and send to support for additional assistance. References: • Reviewing the Service Version and Status Using the SYSTEM HEALTH Tab, on page 53 • Creating a Support File for a Single Host , on page 29
Unable to log into the controller GUI after an apparently successful installation.	Network connectivity to the controller is failing.	Review and test your network connections to the controller. Reference: • Confirming Network Access to the Controller, on page 17

Symptom	Possible Cause	Recommended Action
Unable to update Cisco APIC-EM using the recommended standard methods.		Run the *apply_update* script. Reference: • Updating Cisco APIC-EM Using the Apply Update Script, on page 19 **Important** For additional detailed information about updating the Cisco APIC-EM, as well as additional recovery procedures for a failed update, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*.

Confirming Network Access to the Controller

After a Cisco APIC-EM installation, if you are unable to log into and view the controller's GUI, then perform the following troubleshooting activities:

- Use the **ping** command to see if you can communicate with the host. Run the **ping** command with the host's IP address to test network access to the controller.
- If your deployment is a multi-host deployment, then use the **ping** command to see if you can communicate with any of the other hosts in the multi-host cluster. Run the **ping** command with the other host IP addresses to test network access.
- If the **ping** command fails or timeouts, then there may be an issue with the network values entered during the controller installation. Proceed to review the network access to the controller and the network values entered using the configuration wizard. To review the network values entered during installation with the configuration wizard, re-run the configuration wizard using the **config_wizard** command. For information about this procedure, see Updating the Configuration Using the Wizard, on page 24.

  Ensure that the following network values have been configured correctly:

  - Default gateway address (if this exists)
  - DNS server address
  - NTP server address

Confirming that Core Services are Running

If you are unable to access the Cisco APIC-EM GUI or for any other issues, then you can use the Cisco APIC-EM CLI to check for faulty or failed services.

Before You Begin

You should have attempted to install the Cisco APIC-EM following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the following command to display the status of the core services:

```
$ sudo service grapevine status
```

Step 4 Enter your password a second time when prompted.

```
$[sudo] password for grapevine: ********
```

Command output similar to the following should appear. The core services should have a RUNNING status.

```
grapevine is running
grapevine_capacity_manager              RUNNING   pid 5951, uptime 18:13:31
grapevine_capacity_manager_lxc_plugin   RUNNING   pid 5956, uptime 18:13:31
grapevine_cassandra                     RUNNING   pid 5952, uptime 18:13:31
grapevine_client                        RUNNING   pid 5949, uptime 18:13:31
grapevine_coordinator_service           RUNNING   pid 5958, uptime 18:13:31
grapevine_dlx_service                   RUNNING   pid 5954, uptime 18:13:31
grapevine_log_collector                 RUNNING   pid 5959, uptime 18:13:31
grapevine_root                          RUNNING   pid 5953, uptime 18:13:31
grapevine_supervisor_event_listener     RUNNING   pid 5948, uptime 18:13:31
grapevine_ui                            RUNNING   pid 6084, uptime 18:13:30
reverse-proxy=4.0.0.10000               RUNNING   pid 11630, uptime 18:10:15
router=4.0.0.10000                      RUNNING   pid 11631, uptime 18:10:15
(grapevine)
```

Step 5 If any of the core services are not in the RUNNING state, enter the root cause analysis (rca) command.

```
$ rca
```

The **rca** command runs a root cause analysis script that creates a `tar` file that contains the following data:

- Log files
- Configuration files

- Command output

Note For a multi-host deployment (three hosts), you need to perform this procedure and run the **rca** command on each of the three hosts.

Step 6 Send the `tar` file created by the **rca** command procedure to Cisco support for assistance in resolving your issue. For information about contacting Cisco support, see Contacting the Cisco Technical Assistance Center, on page 87.

Updating Cisco APIC-EM Using the Apply Update Script

If you are unable to update Cisco APIC-EM using the recommended standard methods due to the fact that the controller's GUI is inaccessible or the **grape update upload** command is not working (when using the CLI to upgrade the controller as described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*), then use the procedure described below. This procedure involves using the *apply_update* script.

Note If you are encountering errors after the upload process is completed (during the subsequent verification process or after the verification procedure), then running the *apply_update* script in this procedure will not solve the problem. This script is only provided as a workaround for issues encountered during the upload process.

Important The script should only be used when the recommended, standard methods to upload and update the controller are not working. This script should not be used as an alternative method.

Before You Begin

You have installed the Cisco APIC-EM following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Note With most of the Cisco APIC-EM releases, the *apply_update* script is packaged with the Cisco APIC-EM itself and accessible within the host after installation. In the following releases though, you need to first download the script from the Download Software link:

- 1.0.2.8
- 1.0.3.4

For information about downloading and updating the controller on these releases with the *apply_update* script, see Updating Cisco APIC-EM Using the Apply Update Script (Releases 1.0.2.8, 1.0.3.4), on page 21

Step 1 Review the information in the Cisco notification about the Cisco APIC-EM upgrade.
The Cisco notification specifies the location of the release upgrade pack and verification values for either a Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) 512 bits (SHA512) checksum.

Note The Cisco APIC-EM release upgrade pack is a bit file that varies in size based upon the requirements of the specific upgrade. The release upgrade pack can be as large as several Gigabits.

Step 2 Download the Cisco APIC-EM upgrade package from the Cisco website at the Download Software link.
The release upgrade pack is available for download as a tar file that is also compressed, so the release upgrade pack has a .tar.gz extension. The release upgrade pack itself may consist of any or all of the following update files:

- Service files
- Grapevine files
- Linux files

Note Each release upgrade pack contains an encrypted Cisco signature for security purposes, as well as release version metadata that validates the package.

Step 3 Run a checksum against the file using your own checksum verification tool or utility (either MD5 or SHA512).

Step 4 Review the displayed checksum verification value from your checksum verification tool or utility.
If the output from your checksum verification tool or utility matches the appropriate checksum value in the Cisco notification or from the Cisco secure website, then proceed to the next step. If the output does not match the checksum value, then download the release upgrade pack and perform another checksum. If checksum verification issues persist, contact Cisco support.

Step 5 Copy or move the file from your laptop or secure network location to the appliance, server, or virtual machine with the controller.

Step 6 Using a Secure Shell (SSH) client, log into the host (appliance, server or virtual machine) with the IP address that you specified using the configuration wizard.

Step 7 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 8 Navigate to the folder where the file is located and run the following command:

```
$ sudo /opt/cisco/grapevine/bin/apply_update [path-to-upgrade-file]
```

Note The script is located on /opt/cisco/grapevine/bin/apply_update, but you can run the script from anywhere on the cluster.

What to Do Next

Review the command output. If the upload is successful, then the update process will immediately follow.

If the script fails for any reason, then contact Cisco support for additional steps to take.

Updating Cisco APIC-EM Using the Apply Update Script (Releases 1.0.2.8, 1.0.3.4)

If you are unable to update Cisco APIC-EM using the recommended standard methods due to the fact that the controller's GUI is inaccessible or the **grape update upload** command is not working (when using the CLI to upgrade the controller as described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*), then use the procedure described below. This procedure involves using the *apply_update* script.

Note If you are encountering errors after the upload process is completed (during the subsequent verification process or after the verification process), then running the *apply_update* script in this procedure will not solve the problem. This script is only provided as a workaround for issues encountered during the upload process.

Important The script should only be used when the recommended, standard methods to upload and update the controller are not working. This script should not be used as an alternative method.

Before You Begin

You have installed the Cisco APIC-EM following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

With most of the Cisco APIC-EM releases, the *apply_update* script is packaged with the Cisco APIC-EM itself and accessible within the host after installation. In the following releases though, you need to also download the script from the Download Software link:

- 1.0.2.8
- 1.0.3.4

Step 1 Determine that your controller's Cisco APIC-EM release version is either 1.0.2.8 or 1.0.3.4.
Access the controller's GUI and review the release version on the **Home** page.

Important This procedure should only be performed on controllers running those release versions.

Step 2 Access the download page for Cisco APIC-EM releases located at the Download Software link.

Step 3 Download the script called *apply_update*.

Step 4 Using a Secure Shell (SSH) client, log into the host (appliance, server or virtual machine) with the IP address that you specified using the configuration wizard.

Step 5 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 6 Using SCP or another secure method, copy the *apply_update* script to the Grapevine root for your cluster.

Step 7 Next, review the information in the Cisco notification about the Cisco APIC-EM upgrade.
The Cisco notification specifies the location of the release upgrade pack and verification values for either a Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) 512 bits (SHA512) checksum.

Note The Cisco APIC-EM release upgrade pack is a bit file that varies in size based upon the requirements of the specific upgrade. The release upgrade pack can be as large as several Gigabits.

Step 8 Download the Cisco APIC-EM upgrade package from the Cisco website at the Download Software link.
The release upgrade pack is available for download as a tar file that is also compressed, so the release upgrade pack has a .tar.gz extension. The release upgrade pack itself may consist of any or all of the following update files:

- Service files
- Grapevine files
- Linux files

Note Each release upgrade pack contains an encrypted Cisco signature for security purposes, as well as release version metadata that validates the package.

Step 9 Run a checksum against the file using your own checksum verification tool or utility (either MD5 or SHA512).

Step 10 Review the displayed checksum verification value from your checksum verification tool or utility.
If the output from your checksum verification tool or utility matches the appropriate checksum value in the Cisco notification or from the Cisco secure website, then proceed to the next step. If the output does not match the checksum value, then download the release upgrade pack and perform another checksum. If checksum verification issues persist, contact Cisco support.

Step 11 Copy or move the file from your laptop or secure network location to the appliance, server, or virtual machine with the controller.

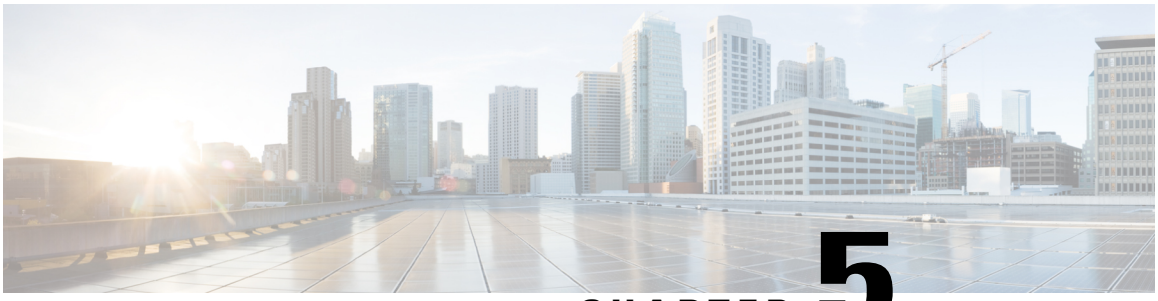
Step 12 Run the script on the Grapevine root with root permissions on the upgrade file. For example, run the following command:

```
$ sudo ./apply_update [path-to-upgrade-file]
```

What to Do Next

Review the command output. If the upload is successful, then the update process will immediately follow.

If the script fails for any reason, then contact Cisco support for additional steps to take.



CHAPTER 5

Troubleshooting the Configuration

The following information may be used to troubleshoot issues with the configuration:

- Troubleshooting the Configuration, page 23
- Updating the Configuration Using the Wizard, page 24
- Resetting the Cisco APIC-EM, page 25
- Restoring the Controller to the Factory Default, page 27
- Creating a Support File for a Single Host , page 29

Troubleshooting the Configuration

The following table describes recommended actions to take to resolve a Cisco APIC-EM configuration issue.

Symptom	Possible Cause	Recommended Action
Controller in a *single-host* configuration appears to be in an unstable state. For example, applications are not running, or applications are inaccessible, and/or not appearing in the GUI.	Controller in unstable state, possibly due to error(s) in entering configuration values with the Cisco APIC-EM configuration wizard.	Log into the host, check the configuration values, and reenter any configuration values that are incorrect. References: • Updating the Configuration Using the Wizard, on page 24

Symptom	Possible Cause	Recommended Action
Controller in a *multi-host* configuration appears to be in an unstable state. For example, applications are not running, or applications are inaccessible, and/or not appearing in the GUI.	Controller in unstable state, possibly due to error(s) in entering configuration values with the Cisco APIC-EM configuration wizard.	Log into the host, check the configuration values, and reenter any configuration values that are incorrect. References: • Changing the Settings in a Multi-Host Cluster, on page 49
Controller was working fine for a period of time after its initial deployment, but then lapses into an unstable state. For example, applications are not running, or applications are inaccessible, and/or not appearing in the GUI.	Possible user or other error in configuration values that occurs after the initial deployment.	Revert back to the first configuration or the factory default configuration. References: • Resetting the Cisco APIC-EM, on page 25 • Restoring the Controller to the Factory Default, on page 27
Controller was working fine for a multi-host configuration, but after a period of time one of the hosts becomes erratic and unstable.	Possible failed service or services in the multi-host cluster.	Remove and then reattach unstable host from the multi-host cluster. References: • Removing a Single Host from a Multi-Host Cluster , on page 36
Controller was working fine for a multi-host configuration, but after a period of time one of the hosts *fails*.	Possible failed service or services in the multi-host cluster.	Remove and then reattach failed and inoperable host from the multi-host cluster. References: • Removing a Faulted Host from a Multi-Host Cluster, on page 37

Updating the Configuration Using the Wizard

You can troubleshoot the Cisco APIC-EM deployment by running the configuration wizard a second time and updating any earlier configuration entries. The configuration wizard saves and displays your previous configuration settings, so you do not have to reenter them.

Note When performing this procedure, controller downtime occurs. For this reason, we recommend that you perform this procedure during a maintenance time period. For information about changing settings for a multi-host configuration, see Changing the Settings in a Multi-Host Cluster, on page 49.

Before You Begin

You have installed the Cisco APIC-EM following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Restart the configuration wizard using the following command.

```
$ config_wizard
```

Note The **config_wizard** command is in the PATH of the 'grapevine' user, and not the "root" user. Either run the command as the "grapevine" user, or fully qualify the command as the "root" user. For example: **/home/grapevine/bin/config_wizard**

Step 4 Review the current configuration values in the configuration wizard and click **next>>**, until you access the specific step where you wish to update your previous configuration entry.
For example, if you need to enter a new NTP server IP address, click **next >>** until you get to the **NTP SERVER SETTINGS** screen.

Step 5 Update the value that was previously entered in the configuration wizard and is currently displayed.
For example, you can update the NTP server settings by entering a new IP address.

Step 6 Click **next>>** until the last step of the configuration wizard process.

Step 7 Click **proceed>>** to have the configuration wizard save and apply your configuration changes to your Cisco APIC-EM deployment.

Resetting the Cisco APIC-EM

You can troubleshoot a Cisco APIC-EM deployment by resetting the controller back to configuration values that were originally set using the configuration wizard the first time. A reset of the controller is helpful, when the controller has gotten itself into an unstable state and other troubleshooting activities have not resolved the situation.

Note In a multi-host environment, you need to perform this procedure on only a single host. After performing this procedure on a single host, the other two hosts will be automatically reset.

Before You Begin

You have installed the Cisco APIC-EM following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Navigate to the `bin` directory on the Grapevine root. The `bin` directory contains the grapevine scripts.

Step 4 Enter the **reset_grapevine** command at the prompt to run the reset grapevine script.

```
$ reset_grapevine
```

The **reset_grapevine** command returns the configuration settings back to values that you configured when running the configuration wizard for the first time. The configuration settings are saved to a .JSON file. This .JSON file is located at: `/etc/grapevine/controller-config.json`. The **reset_grapevine** command uses the data in the `controller-config.json` file to return to the earlier configuration settings, so do not delete this file. If you delete this file, you must run the configuration wizard again and reenter your configuration data.

Important The **reset_grapevine** command will terminate if the SSH connection is disconnected for any reason. To avoid this, we recommend that you use tmux (terminal multiplexer) which is already installed on the controller to run the **reset_grapevine** command in the session. You can use the following commands for tmux:

tmux new -s *session_name* **reset_grapevine**	Command to create a new session using tmux for reset-grapevine. For example, you can enter the following command: **tmux new -s** *session100* **reset_grapevine**
tmux ls	Command to view a the list of tmux sessions.
tmux attach -t *session_name* **reset_grapevine**	Command to attach to a tmux session. For example, you can enter the following command: **tmux attach -t** *session200* **reset_grapevine** To get more information about tmux, you can run the **man tmux** command.

After entering the **reset_grapevine** command, you are then prompted to reenter your Grapevine password.

Step 5 Enter your Grapevine password a second time.

```
[sudo] password for grapevine:********
```

You are then prompted to delete all virtual disks The virtual disks are where the Cisco APIC-EM database resides. For example, data about devices that the controller discovered are saved on these virtual disks. If you enter yes (**y**), all of this data is deleted. If you enter no (**n**), then the new cluster will come up populated with your existing data once the reset procedure completes.

Step 6 Enter **n** to prevent the deletion all of the virtual disks.

```
THIS IS A DESTRUCTIVE OPERATION
Do you want to delete all VIRTUAL DISKS in your APIC-EM cluster? (y/n):n
```

You are then prompted to delete all Cisco APIC-EM authentication timeout policies, user password policies, and user accounts other than the primary administrator account.

Step 7 Enter **n** to prevent the deletion of all authentication timeout policies, user password policies, and user accounts other than the primary administrator account.

```
THIS IS A DESTRUCTIVE OPERATION
Do you want to delete authentication timeout policies, user password policies,
and Cisco APIC-EM user accounts other than the primary administrator account? (y/n): n
```

You are then prompted to delete any imported certificates.

Step 8 Enter **n** to prevent the deletion of any imported certificates.

```
THIS IS A DESTRUCTIVE OPERATION
Do you want to delete the imported certificates? (y/n): n
```

You are then prompted to delete any backups.

Step 9 Enter **n** to prevent the deletion of any backups.

```
THIS IS A DESTRUCTIVE OPERATION
Do you want to delete the backups? (y/n): n
```

The controller then resets itself with the configuration values that were originally set using the configuration wizard the first time. When the controller is finished resetting, you are presented with a command prompt from the controller.

Step 10 Using the Secure Shell (SSH) client, log out of the host.

Restoring the Controller to the Factory Default

In certain situations, you may want to restore the Cisco APIC-EM to its original factory default settings. For example, if your controller appliance is being replaced or simply has an undesirable configuration that needs to be completely removed. Under these circumstances, you can restore the controller to its factory defaults and then proceed to reconfigure it as a new controller.

This procedure describes how to a restore the factory defaults to the controller.

Caution This procedure shuts down both the Cisco APIC-EM and the host (physical or virtual) on which it resides. At the end of this procedure, you will need to access the host and restart it.

Before You Begin

You have installed the Cisco APIC-EM following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

You have access to the Cisco APIC-EM using either a physical console or a Telnet connection.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the **reset_grapevine factory** command at the prompt.

```
$ reset_grapevine factory
```

Important The **reset_grapevine factory** command will terminate if the SSH connection is disconnected for any reason. To avoid this, we recommend that you use tmux (terminal multiplexer) which is already installed on the controller to run the **reset_grapevine factory** command in the session. You can use the following commands for tmux:

tmux new -s *session_name* **'reset_grapevine factory'**	Command to create a new session using tmux for reset-grapevine factory. Note that 'reset-grapevine factory' in this command is a string value and therefore must be entered within single quotation marks. For example, you can enter the following command: **tmux new -s** *session100* **'reset_grapevine factory'**
tmux ls	Command to view a the list of tmux sessions.
tmux attach -t *session_name* **'reset_grapevine factory'**	Command to attach to a tmux session. Note that 'reset-grapevine factory' in this command is a string value and therefore must be within single quotation marks. For example, you can enter the following command: **tmux attach -t** *session200* **'reset_grapevine factory'** To get more information about tmux, you can run the **man tmux** command.

Step 4 Enter your Linux grapevine password a second time to start the reset process.

```
$ sudo password for grapevine *********
```

After entering this command a warning appears that the **reset_grapevine factory** command will shut down the controller.

You are then prompted to confirm your desire to run the **reset_grapevine factory** command.

Step 5 Enter **Yes** to confirm that you want to run the **reset_grapevine factory** command.
The controller then performs the following tasks:

- Stops all running clients and services
- Deletes all cluster data
- Deletes all user data
- Deletes the configuration files including secrets and private keys
- Shuts down the controller
- Shuts down the host (physical or virtual)

What to Do Next

Perform the following tasks:

- Start up the host (physical or virtual).
- After start up, the configuration wizard appears and prompts you to re-deploy the Cisco APIC-EM.
- Proceed to re-deploy the Cisco APIC-EM using the configuration wizard.

Creating a Support File for a Single Host

You can troubleshoot the Cisco APIC-EM deployment by creating a root cause analysis (rca) support file. This rca file consists of logs, configuration files, and command output. After you create this rca file, you can then email it to Cisco support for assistance.

Before You Begin

You have installed the Cisco APIC-EM following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Navigate to the `bin` directory on the host. The `bin` directory contains the grapevine scripts.

Step 4 To create the support file, enter the **rca** command in this directory.

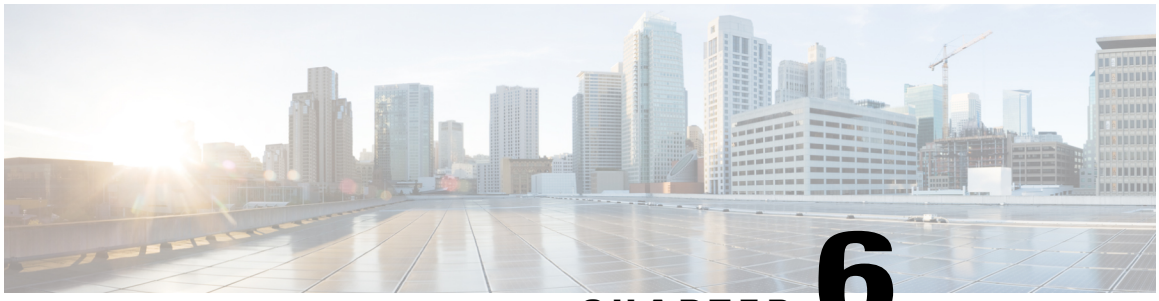
```
$ rca
[sudo] password for grapevine:
mkdir: created directory '/tmp/grapevine-root-172.24.100.15-rca-2016-08-05_18-17-04_UTC+0000'
============================================================
RCA package created on Fri Aug  5 18:17:10 UTC 2016
Max Log Size: 50000000
Skipping collection of ''
============================================================

2016-08-05 18:17:10 | INFO | Generating log for 'date'...
2016-08-05 18:17:10 | INFO | Generating log for 'vmware-toolbox-cmd stat hosttime'...
2016-08-05 18:17:10 | INFO | Generating log for 'vmware-toolbox-cmd stat speed' ..
2016-08-05 18:17:10 | INFO | Generating log for 'vmware-toolbox-cmd stat session id'...
2016-08-05 18:17:10 | INFO | Generating log for 'vmware-toolbox-cmd stat balloon '...
2016-08-05 18:17:10 | INFO | Generating log for 'vmware-toolbox-cmd stat swap'...
2016-08-05 18:17:10 | INFO | Generating log for 'vmware-toolbox-cmd stat memlimit'...
2016-08-05 18:17:10 | INFO | Generating log for 'vmware-toolbox-cmd stat memres'
....
```

The **rca** command runs a root cause analysis script that creates a `tar` file that contains log files, configuration files, and the command output.

Note For a multi-host deployment (three hosts), you need to perform this procedure and run the **rca** command on each of the three hosts. Additionally, if you need to perform a root cause analysis for a specific service, then to identify which host the service is running on, access the controller's GUI, click **admin**, click **System Administration** from the drop down menu, and click **Hosts** at the top of the window to view the individual hosts and their services.

What to Do Next

Send the `tar` file created by this procedure to Cisco support for assistance in resolving your issue. For information about contacting Cisco support, see Contacting the Cisco Technical Assistance Center, on page 87.



CHAPTER 6

Troubleshooting Cisco APIC-EM Single and Multi-Host

The following information may be used to troubleshoot Cisco APIC-EM single and multi-host:

- Recovery Procedures for Cisco APIC-EM Node Failures, page 31
- Removing a Single Host from a Multi-Host Cluster , page 36
- Removing a Faulted Host from a Multi-Host Cluster, page 37
- Resetting the Cisco APIC-EM, page 39
- Adding a New Host to a Multi-Host Cluster, page 41
- Shutting Down and Starting Up a Host in a Multi-Host Cluster, page 45
- Confirming the Multi-Host Cluster Configuration Values, page 47
- Changing the Settings in a Multi-Host Cluster, page 49

Recovery Procedures for Cisco APIC-EM Node Failures

The following table describes recommended procedures to take to resolve a Cisco APIC-EM single node failure scenario.

Table 3: Single Host Recovery Procedures

Node Failure Scenario	Symptoms and Recovery Procedures
Power outage	The node should recover automatically (in most cases) when the power is restored. In rare situations, some of the APIC-EM services may not come up cleanly due to some transient conditions. In such cases, you would need to execute the following steps to ensure that the node comes back online cleanly: **1** If you have not already done so, restart the power on the failed host. **2** Reset the host. See Resetting the Cisco APIC-EM, on page 25.
Bad or faulty hardware	Perform the following steps to recover from a node failure scenario due to bad or faulty hardware: **1** RMA the bad or faulty hardware. **2** Reinstall new hardware. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*. **3** Install Cisco APIC-EM controller software on the new hardware. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*. **4** Restore your database backup using the controller's GUI. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*. **5** Ensure that you have installed and enabled any applications that were previously running on the controller. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*. **6** If applicable to your configuration, add the new host to the cluster. See Adding a New Host to a Multi-Host Cluster, on page 41.

Node Failure Scenario	Symptoms and Recovery Procedures
Controller software upgrade failure	In this case, to recover from the upgrade failure and return to the current Cisco APIC-EM version, perform the following steps: **1** Restore your database backup using the controller's GUI. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*. **2** Ensure that you have installed and enabled any applications that were previously running on the controller. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

The following table describes recommended procedures to resolve a Cisco APIC-EM multi-host (node) failure scenario.

Note When power-cycling Cisco APIC-EM cluster hosts, the recommended procedure is to first power on the host that gets powered off last, and then power on the rest of the hosts, in reverse order (for example, if you first powered down host 1, followed by host 2 and then host 3, then power on host 3, followed by host 2 and then host 1), within 30 seconds.This avoids any possible clustering issues. If this timing recommendation is exceeded, the hosts power-up sequence is not maintained, or any other problem occurs, then the best way to recover is to run the **reset_grapevine** command on one of the hosts in the cluster. When prompted, answer "**n**" to all questions.

Table 4: Multi-Host Recovery Procedures

Node Failure Scenario	Symptoms and Recovery Procedures
Power outage causing one or more of the cluster nodes to go down.	In most cases, the host(s) should rejoin the Cisco APIC-EM cluster on its own when the power is restored. In rare situations, some of the Cisco APIC-EM services may not form the cluster with the existing Cisco APIC-EM hosts. In such cases, you would need to execute the following steps to ensure that the failed host joins the cluster: **1** If you have not already done so, restart the power on the failed host. **2** Reset the host. See Resetting the Cisco APIC-EM, on page 25. **Note** If after a power outage, the host does not come back up, then follow the procedures directly below for recovering from bad or faulty hardware.

Node Failure Scenario	Symptoms and Recovery Procedures
Bad or faulty hardware on one of the cluster nodes.	In this case, you would need to first remove the faulty (bad) host from the cluster and then add the new host to the cluster. Perform the following steps: **1** RMA the bad or faulty hardware. **2** Reinstall new hardware. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*. **3** Install Cisco APIC-EM controller software on the new hardware. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*. **4** Restore your database backup using the controller's GUI. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*. **5** Ensure that you have installed and enabled any applications that were previously running on the controller. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*. **6** Add the new host to the cluster. See Adding a New Host to a Multi-Host Cluster, on page 41.
Network connectivity issues between the cluster nodes.	In most cases, the node(s) should rejoin the Cisco APIC-EM cluster on its own when the network connectivity is restored. In rare situations, some of the Cisco APIC-EM services may not form the cluster with the existing Cisco APIC-EM nodes. In such cases, you would need to execute the following steps to ensure that the failed node joins the cluster: **1** Reset the host. See Resetting the Cisco APIC-EM, on page 25.

Node Failure Scenario	Symptoms and Recovery Procedures
Controller software upgrade failure on one of the cluster hosts.	In this case, to recover from the upgrade failure and return to the current Cisco APIC-EM version, perform the following steps: **1** Restore your database backup using the controller's GUI. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*. **2** Ensure that you have installed and enabled any applications that were previously running on the controller. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.
Hardware upgrade on one of the cluster nodes.	Gracefully, shut down the host, upgrade the hardware (RAM, CPU, etc.) and restart the host. See Shutting Down and Starting Up a Host in a Multi-Host Cluster, on page 45.

Removing a Single Host from a Multi-Host Cluster

To troubleshoot an issue with a multi-host cluster, you may need to remove a single host from a multi-host cluster. This procedure describes how to remove one of the hosts running Cisco APIC-EM from a multi-host cluster. You use the Cisco APIC-EM configuration wizard to perform this procedure.

Note The configuration wizard option to remove a host only appears if the host on which you are running the configuration wizard is part of a multi-host cluster. If the host is not part of a multi-host cluster, then the option to remove a host does not display. When performing this procedure, controller downtime occurs. For this reason, we recommend that you perform this procedure during a maintenance time period.

Before You Begin

You should have installed the Cisco APIC-EM on a multi-host cluster as described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

You must perform this procedure on the single host that is to be removed from the multi-host cluster.

The multi-host cluster should still be operational.

Step 1 Using a Secure Shell (SSH) client, log into the host (appliance, server, or virtual machine) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Note The **config_wizard** command is in the PATH of the 'grapevine' user, and not the "root" user. Either run the command as the "grapevine" user, or fully qualify the command as the "root" user. For example: **/home/grapevine/bin/config_wizard**

Step 4 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the option to remove the host from the cluster:

- **Remove this host from its APIC-EM cluster**

Step 5 A message appears with the following options:

- **[cancel]—**Exit the configuration wizard.
- **[proceed]—**Begin the process to remove this host from its cluster.

Choose **proceed>>** to begin. After choosing **proceed>>**, the configuration wizard begins to remove this host from its cluster.

Step 6 At the end of this process, you must then either run the configuration wizard again to configure the host as a new Cisco APIC-EM or join the Cisco APIC-EM to a cluster.

Important Ensure that you either power off the removed host, restore it to the default factory settings, or do a manual arping to avoid potential virtual IP address conflicts. Before you can use this host as either a standalone controller or operating within a cluster, reinstall the Cisco APIC-EM and run the configuration wizard. Do not attempt to use this host again either as a standalone host or within a cluster without reinstalling the Cisco APIC-EM.

Removing a Faulted Host from a Multi-Host Cluster

Perform the steps in the following procedure to remove a faulted or inoperative host (running Cisco APIC-EM) from a multi-host cluster. You use the Cisco APIC-EM configuration wizard to perform this procedure. A host becomes faulted when it can no longer participate in the cluster due to hardware or software issues.

After following this procedure on a three-host cluster (moving from three hosts to two hosts), you will lose high-availability protection against loss of a host. After following this procedure for a two-host cluster, then the cluster will become inoperable until that second host is brought back up and added to the cluster.

Note The fact that the host becomes "faulted" results in replacement instances of the services on the faulted host being grown on the remaining hosts in the cluster. During the time period when the replacement instances are being grown and depending on the types of services being grown, certain Cisco APIC-EM functionality may not be available.

Before You Begin

You have installed the Cisco APIC-EM on a multi-host cluster following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

You must perform this procedure on an active host in the multi-host cluster. You cannot perform this procedure on the faulted host that is to be removed from the multi-host cluster. A faulted host is displayed as red in the **System Health** tab view in the **Home** page of the controller's GUI.

Note You should always first attempt to bring the faulted host back online. After determining that the faulted host can no longer participate in the cluster, then try to remove the faulted host using the **Remove this host from its APIC-EM cluster** configuration wizard option (as described in the previous procedure). You should only follow this procedure and the **Remove a faulted host from this APIC-EM cluster** configuration wizard option, if that other option is tried first and is unsuccessful in removing the host.

Step 1 Using a Secure Shell (SSH) client, log into the host (appliance, server, or virtual machine) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Note The **config_wizard** command is in the PATH of the 'grapevine' user, and not the "root" user. Either run the command as the "grapevine" user, or fully qualify the command as the "root" user. For example: **/home/grapevine/bin/config_wizard**.

Step 4 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the option to forcibly remove the faulted host from the cluster:

- **Remove a faulted host from this APIC-EM cluster**

Step 5 A message appears with the following options:

- **<Remove *IP Address* from cluster>—**Forcibly removes the faulted host (identified by its IP address) from the multi-host cluster.
- **<exit>—**Exit the configuration wizard without removing the faulted host.

Choose **<Remove *IP Address* from cluster>** to begin. After choosing **<Remove *IP Address* from cluster>**, the configuration wizard begins to remove this faulted host from its cluster.

Step 6 At the end of this process, you must then either run the configuration wizard again to configure the host as a new controller or join the controller to a cluster.

Important Ensure that you either power off the removed host, restore it to the default factory settings, or do a manual arping to avoid potential virtual IP address conflicts. Before you can use this host as either a standalone controller or operating within a cluster, reinstall the Cisco APIC-EM and run the configuration wizard. Do not attempt to use this host again either as a standalone host or within a cluster without reinstalling the Cisco APIC-EM.

Resetting the Cisco APIC-EM

You can troubleshoot a Cisco APIC-EM deployment by resetting the controller back to configuration values that were originally set using the configuration wizard the first time. A reset of the controller is helpful, when the controller has gotten itself into an unstable state and other troubleshooting activities have not resolved the situation.

Note In a multi-host environment, you need to perform this procedure on only a single host. After performing this procedure on a single host, the other two hosts will be automatically reset.

Before You Begin

You have installed the Cisco APIC-EM following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Navigate to the `bin` directory on the Grapevine root. The `bin` directory contains the grapevine scripts.

Step 4 Enter the **reset_grapevine** command at the prompt to run the reset grapevine script.

```
$ reset_grapevine
```

The **reset_grapevine** command returns the configuration settings back to values that you configured when running the configuration wizard for the first time. The configuration settings are saved to a .JSON file. This .JSON file is located at: `/etc/grapevine/controller-config.json`. The **reset_grapevine** command uses the data in the `controller-config.json` file to return to the earlier configuration settings, so do not delete this file. If you delete this file, you must run the configuration wizard again and reenter your configuration data.

Important The **reset_grapevine** command will terminate if the SSH connection is disconnected for any reason. To avoid this, we recommend that you use tmux (terminal multiplexer) which is already installed on the controller to run the **reset_grapevine** command in the session. You can use the following commands for tmux:

tmux new -s *session_name* **reset_grapevine**	Command to create a new session using tmux for reset-grapevine. For example, you can enter the following command: **tmux new -s** *session100* **reset_grapevine**
tmux ls	Command to view a the list of tmux sessions.
tmux attach -t *session_name* **reset_grapevine**	Command to attach to a tmux session. For example, you can enter the following command: **tmux attach -t** *session200* **reset_grapevine** To get more information about tmux, you can run the **man tmux** command.

After entering the **reset_grapevine** command, you are then prompted to reenter your Grapevine password.

Step 5 Enter your Grapevine password a second time.

```
[sudo] password for grapevine:********
```

You are then prompted to delete all virtual disks The virtual disks are where the Cisco APIC-EM database resides. For example, data about devices that the controller discovered are saved on these virtual disks. If you enter yes (**y**), all of this data is deleted. If you enter no (**n**), then the new cluster will come up populated with your existing data once the reset procedure completes.

Step 6 Enter **n** to prevent the deletion all of the virtual disks.

```
THIS IS A DESTRUCTIVE OPERATION
Do you want to delete all VIRTUAL DISKS in your APIC-EM cluster? (y/n):n
```

You are then prompted to delete all Cisco APIC-EM authentication timeout policies, user password policies, and user accounts other than the primary administrator account.

Step 7 Enter **n** to prevent the deletion of all authentication timeout policies, user password policies, and user accounts other than the primary administrator account.

```
THIS IS A DESTRUCTIVE OPERATION
Do you want to delete authentication timeout policies, user password policies,
and Cisco APIC-EM user accounts other than the primary administrator account? (y/n): n
```

You are then prompted to delete any imported certificates.

Step 8 Enter **n** to prevent the deletion of any imported certificates.

```
THIS IS A DESTRUCTIVE OPERATION
Do you want to delete the imported certificates? (y/n): n
```

You are then prompted to delete any backups.

Step 9 Enter **n** to prevent the deletion of any backups.

```
THIS IS A DESTRUCTIVE OPERATION
Do you want to delete the backups? (y/n): n
```

The controller then resets itself with the configuration values that were originally set using the configuration wizard the first time. When the controller is finished resetting, you are presented with a command prompt from the controller.

Step 10 Using the Secure Shell (SSH) client, log out of the host.

Adding a New Host to a Multi-Host Cluster

Perform the steps in this procedure to configure Cisco APIC-EM on your host and to join it to another, pre-existing host to create a cluster. Configuring the Cisco APIC-EM on multiple hosts to create a cluster is best practice for both high availability and scale.

⚠

Caution

- When joining a host to a cluster as described in the procedure below, there is no merging of the data on the two hosts. The data that currently exists on the host that is joining the cluster is erased and replaced with the data that exists on the cluster that is being joined to.
- When joining the additional hosts to form a cluster be sure to join only a single host at a time. You should not join multiple hosts at the same time, as doing so will result in unexpected behavior.
- You should also expect some service downtime when the adding or removing hosts to a cluster, since the services are then redistributed across the hosts. Be aware that during the service redistribution, there will be downtime.

Before You Begin

You must have performed the following prerequisites:

- You must have either received a Cisco APIC-EM Controller Appliance with the Cisco APIC-EM pre-installed or you must have downloaded, verified, and installed the Cisco ISO image onto a second server or virtual machine.
- You must have already configured Cisco APIC-EM on the first host (server or virtual machine) in your planned multi-host cluster following the steps in the previous procedure.
- Additionally, you must have checked the controller's health on the first host using the **SYSTEM HEALTH** tab in the GUI. The **SYSTEM HEALTH** tab is directly accessible from the **HOME** page. For information

about this procedure, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

This procedure must be run on the second host that you are joining to the cluster. When joining the new host to the cluster, you must specify an existing host in the cluster to connect to.

Note The Cisco APIC-EM multi-host configuration supports the following two workflows:

- You first configure a single host running Cisco APIC-EM in your network. After performing this procedure, you then use the wizard to configure and join two additional hosts to form a cluster.
- If you already have several single hosts configured with Cisco APIC-EM, you can use the configuration wizard to join two additional hosts to a single host to form a cluster.

Step 1 Boot up the host.

Step 2 Review the **APIC-EM License Agreement** screen that appears and choose either **<view license agreement>** to review the license agreement or **accept>>** to accept the license agreement and proceed with the deployment.

Note You will not be able to proceed without accepting the license agreement.

After accepting the license agreement, you are then prompted to select a configuration option.

Step 3 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose one of the two displayed options to begin.

- **Create a new APIC-EM cluster**
- **Add this host to an existing APIC-EM cluster**

For the multi-host deployment, click the **Add this host to an existing APIC-EM cluster** option.

Step 4 Enter configuration values for the **NETWORK ADAPTER #1** on the host.
The configuration wizard discovers and prompts you to confirm values for the network adapter or adapters on your host. For example, if your host has two network adapters you are prompted to confirm configuration values for network adapter #1 (eth0) and network adapter #2 (eth1).

Note

Important On Cisco UCS servers, the NIC labeled with number 1 would be the physical NIC. The NIC labeled with the number 2 would be eth1.

Host IP address	Enter a host IP address to use for the network adapter. This host IP address connects to the external network or networks. **Note** The network adapter(s) connect to the external network or networks. These external network(s) consists of the network devices, NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI.

Netmask	Enter the netmask for the network adapter's IP address.

Later in this procedure, the following information will be discovered and copied from the cluster to the configuration file of this host:

- Default Gateway IP address
- DNS Servers
- Static Routes

Once satisfied with the controller network adapter settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered. After validation, you are then prompted to enter values for the **APIC-EM CLUSTER SETTINGS**.

Step 5 Enter configuration values for the **APIC-EM CLUSTER SETTINGS**.

Remote Host IP	Enter the eth0 IP address of the pre-configured host that you are now joining to form a cluster. **Note** If a virtual IP address has already been configured on another host for a multi-host cluster, you may also enter that IP address value. This field accepts either the IP address of a pre-configured host to the cluster or the virtual IP address of the cluster.
Administrator Username	Enter an administrator username. This is the administrator username on the pre-configured host that you are now joining to form a cluster.
Administrator Password	Enter an administrator password. This is the administrator password on the pre-configured host that you are now joining to form a cluster. For information about the requirements for an administrator password, see the Password Requirements section in Chapter 2, Securing the Cisco APIC-EM in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*. **Note** The administrator password is encrypted and hashed in the controller database.

After configuring the administrator cluster settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard then proceeds to prepare the host to join the cluster.

You will receive a message to please wait, while the remote cluster is being queried and data is retrieved.

Step 6 Enter configuration values for the **Virtual IP**.

Note If you are joining the host to a cluster where the virtual IP has already been configured, then you will not be prompted for virtual IP configuration values. If you are joining the host to a cluster where a virtual IP has not yet been configured, then you will be prompted for virtual IP configuration values.

Virtual IP	Enter the virtual IP address to use for the network that the controller is directed to. **Note** For additional information about virtual IP, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Once satisfied with the virtual IP address settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered.

Step 7 (Optional) Enter additional configuration values for the **Virtual IP**.
The configuration wizard proceeds to continue its discovery of any pre-existing configuration values on the hosts in the cluster. Depending upon what the configuration wizard discovers, you may be prompted to enter additional configuration values. For example:

- If eth1 was configured on a pre-existing host in the cluster, then you are prompted to enter the host IP address that was configured for eth1. You are also prompted for a VIP, if it has not yet been configured for this NIC.
- If eth2 was configured on a pre-existing host in the cluster, then you are prompted to enter the host IP address that was configured for eth2. You are also prompted for a VIP, if it has not yet been configured for this NIC.
- If eth3 was configured on a pre-existing host in the cluster, then you are prompted to enter the host IP address that was configured for this eth3. You are also prompted for a VIP, if it has not yet been configured for this NIC.

Note This configuration wizard discovery process and prompting continues for the number of configured Ethernet ports in the cluster.

Virtual IP	Enter the virtual IP address to use for the network that the controller is directed to.
IP address	Enter an IP address to use for this network adapter. This IP address connects to the external network or networks. **Note** The network adapter(s) connect to the external network or networks. These external network(s) consists of the network devices, NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI.

Once satisfied with the virtual IP address settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered.

Step 8 A final message appears stating that the wizard is now ready to proceed to join the host to the cluster.
The following options are available:

- **[back]—**Review and verify or modify your configuration settings.
- **[cancel]—**Discard your configuration settings and exit the configuration wizard.
- **[proceed]—**Save your configuration settings and begin the process to join this host to the specified Cisco APIC-EM.

Enter **proceed>>** to proceed. After entering **proceed>>**, the configuration wizard applies the configuration values that you entered above.

Note

At the end of the configuration process, a successful configuration message appears.

Step 9 Open your browser and enter an IP address to access the Cisco APIC-EM GUI.
You can use the first displayed IP address of the Cisco APIC-EM GUI at the end of the configuration process.

Note The first displayed IP address can be used to access the Cisco APIC-EM GUI. The second displayed IP address accesses the network where the devices reside.

Step 10 After entering the IP address in the browser, a message stating that "Your connection is not private" appears.
Ignore the message and click the **Advanced** link.

Step 11 After clicking the **Advanced** link, a message stating that the site's security certificate is not trusted appears.
Ignore the message and click the link.

Note This message appears because the controller uses a self-signed certificate. You will have the option to upload a trusted certificate using the controller GUI after installation completes.

Step 12 In the **Login** window, enter the administrator username and password that you configured above and click the **Log In** button.

What to Do Next

Proceed to follow the same procedure described here to join the third and final host to the multi-host cluster.

After configuring each host be sure to check the controller's health on the host using the **SYSTEM HEALTH** tab in the GUI. The **SYSTEM HEALTH** tab is directly accessible from the **HOME** page. For information about this procedure, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Note You can send feedback about the Cisco APIC-EM by clicking the Feedback icon ("I wish this page would....") at the lower right of each window in the GUI. Clicking on this icon opens an email. Use this email to send a comment on the current window or to send a request to the Cisco APIC-EM development team.

Shutting Down and Starting Up a Host in a Multi-Host Cluster

Perform the steps in this procedure to gracefully shutdown and restart a host in a multi-host cluster.

Note It is best practice to gracefully shutdown a host, before removing it from the multi-host cluster.

Before You Begin

You should have installed the Cisco APIC-EM on a multi-host cluster as described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

You must perform this procedure on the single host that is to be removed from the multi-host cluster.

The multi-host cluster should still be operational.

Step 1 Using a Secure Shell (SSH) client, log into the host (appliance, server, or virtual machine) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the following command to redeploy services off of this host and onto the other hosts in the multi-host cluster.

```
$ grape host evacuate
```

Step 4 Power off the host.

Step 5 Proceed to perform any troubleshooting or maintenance operations on the host that you powered off.

Step 6 Power on the host back on.

Step 7 If the hosts comes up and no error message appears, then enter the following command on the host to enable services on it.

```
$ grape host enable
```

Note If the host fails to come up, then proceed directly to step 9 below.

Step 8 If the hosts comes up and no error message appears, then enter the following additional command on the host to rebalance services on it and with other hosts in your multi-host cluster.

```
$ grape instance rebalance
```

Note If the hosts comes up and no error message appears, then you are finished with the procedure. If the host fails to come up, then proceed directly to step 9 below.

Step 9 Log into one of the other operational hosts (working hosts) in the multi-host cluster.

Step 10 Enter the following command on the selected operational host.

```
$ remove faulted node
```

This command will remove the stale entries of the host that was shut down.

Step 11 Run the configuration wizard on the selected operational node to trigger 'remove fault-node node'.

```
$ config_wizard
```

Step 12 The operational host will then display another selection, 'Revert to single-node',

Step 13 Select the 'Revert to single-node' option and wait until operation completes.

Step 14 Proceed to join the host back to the existing two host cluster using the configuration wizard and as described in the procedure to add a host to a multi-host cluster. For information, see Adding a New Host to a Multi-Host Cluster, on page 41.

Confirming the Multi-Host Cluster Configuration Values

If you are experiencing issues with your multi-host cluster, then you can use the Cisco APIC-EM CLI to check the configuration values.

Before You Begin

You should have installed the Cisco APIC-EM following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the following command to display the multi-host configuration.

```
$ grape root display
```

Command output similar to the following should appear.

```
ROOT                                    PROPERTY             VALUE
------------------------------------------------------------------------

4cbe3972-9872-4771-800d-08c89463f1eb   hostname             root-1
4cbe3972-9872-4771-800d-08c89463f1eb   interfaces           [{'interface': 'eth0', 'ip':
'209.165.200.10', 'mac': '00:50:56:100:d2:14', 'netmask': '255.255.255.0'}, {'interface': 'eth1',
'ip': '209.165.200.10', 'mac': '00:50:56:95:5c:18', 'net  mask': '255.255.255.0'}, {'interface':
'grape-br0', 'ip': '209.165.200.11', 'mac': 'ba:ed:c4:19:0d:77', 'netmask': '255.255.255.0'}]
4cbe3972-9872-4771-800d-08c89463f1eb   is_alive             True
4cbe3972-9872-4771-800d-08c89463f1eb   last_heartbeat       Wed Sep 09, 2015 11:02:52 PM (just now)

4cbe3972-9872-4771-800d-08c89463f1eb   public_key           ssh-rsa

c2EAAAADAQABAAABAQDYlyCfidke3MTjGkzsTAu73MtG+lynFFvxWZ4xVIkDkhGC7KCs6XMhORMaABb6
bU4EX/6osa4qyta4NYaijxjL6GL6kPkSBZiEKcUekHCmk1+H+Ypp5tc0wyvSpe5HtbLvPicLrXHHI/TS
...
V44t+VvtFaLurG9+FW/ngZwGrR/grapevine@grapevine-root

4cbe3972-9872-4771-800d-08c89463f1eb   root_id              4cbe3972-9872-4771-800d-08c89463f1eb
4cbe3972-9872-4771-800d-08c89463f1eb   root_index           0
4cbe3972-9872-4771-800d-08c89463f1eb   root_version         0.3.0.958.dev140-gda6a16
4cbe3972-9872-4771-800d-08c89463f1eb   vm_password          ******
(grapevine)

#

ROOT                                    PROPERTY             VALUE
------------------------------------------------------------------------
```

```
4cbe3972-9872-4771-800d-08c89463f1eb   hostname             root-2
4cbe3972-9872-4771-800d-08c89463f1eb   interfaces           [{'interface': 'eth0', 'ip':
'209.165.200.101, 'mac': '00:50:56:100:d2:14', 'netmask': '255.255.255.0'}, {'interface': 'eth1',
'ip': '209.165.200.11', 'mac': '00:50:56:95:5c:18', 'net  mask': '255.255.255.0'}, {'interface':
'grape-br0', 'ip': '209.165.200.11', 'mac': 'ba:ed:c4:19:0d:77', 'netmask': '255.255.255.0'}]
4cbe3972-9872-4771-800d-08c89463f1eb   is_alive             True
4cbe3972-9872-4771-800d-08c89463f1eb   last_heartbeat       Wed Sep 09, 2015 11:02:52 PM (just now)

4cbe3972-9872-4771-800d-08c89463f1eb   public_key           ssh-rsa

c2EAAAADAQABAAABAQDYlyCfidke3MTjGkzsTAu73MtG+lynFFvxWZ4xVIkDkhGC7KCs6XMhORMaABb6
bU4EX/6osa4qyta4NYaijxjL6GL6kPkSBZiEKcUekHCmk1+H+Ypp5tc0wyvSpe5HtbLvPicLrXHHI/TS
...
V44t+VvtFaLurG9+FW/ngZwGrR/grapevine@grapevine-root

4cbe3972-9872-4771-800d-08c89463f1eb   root_id              4cbe3972-9873-4771-800d-08c89463f1eb
4cbe3972-9872-4771-800d-08c89463f1eb   root_index           0
4cbe3972-9872-4771-800d-08c89463f1eb   root_version         0.3.0.958.dev140-gda6a16
4cbe3972-9872-4771-800d-08c89463f1eb   vm_password          ******
(grapevine)
```

The following data is displayed by this command:

- `hostname`—The configured hostname.
- `interfaces`—The configured interface values, including Ethernet port, IP address, and netmask.
- `is_alive`—Status of the host. `True` indicates a running host, `False` indicates a host that has shut down.
- `last_heartbeat`—Date and time of last heartbeat message sent from the host.
- `public_key`—Public key used by host.
- `root_id`—Individual root identification number.
- `root_index`—Individual root index number.
- `root_version`—Software version of root.
- `vm_password`—VMware vSphere password that is masked.

Step 4 If any of the fields in the command output appear incorrect, enter the root cause analysis (rca) command.

```
$ rca
```

The **rca** command runs a root cause analysis script that creates a `tar` file that contains the following data:

- Log files
- Configuration files
- Command output

Note For a multi-host deployment (three hosts), you need to perform this procedure and run the **rca** command on each of the three hosts.

Step 5 Send the `tar` file created by the **rca** command procedure to Cisco support for assistance in resolving your issue.

For information about contacting Cisco support, see Contacting the Cisco Technical Assistance Center, on page 87.

Changing the Settings in a Multi-Host Cluster

To troubleshoot an issue with a multi-host cluster, you may need to change its configuration settings. This procedure describes how to change the Cisco APIC-EM external network settings, NTP server address, and/or password for the Linux grapevine user in a multi-host cluster. The external network settings that can be changed include:

- Host IP address
- Virtual IP address
- DNS server
- Default gateway
- Static routes

Note In order to change the external network settings, NTP server address, and/or the Linux grapevine user password in a multi-host deployment, you need to first break up the multi-host cluster. As a result, controller downtime occurs. For this reason, we recommend that you perform this procedure during a maintenance time period. For information about changing settings for a single-host configuration, see Updating the Configuration Using the Wizard, on page 24

Before You Begin

You must have successfully configured the Cisco APIC-EM as a multi-host cluster using the configuration wizard, as described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Step 1 Using a Secure Shell (SSH) client, log into one of the hosts in your cluster.
Log in using the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Note The **config_wizard** command is in the PATH of the 'grapevine' user, and not the "root" user. Either run the command as the "grapevine" user, or fully qualify the command as the "root" user. For example: **/home/grapevine/bin/config_wizard**

Step 4 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the option to remove the host from the cluster:

- **Remove this host from its APIC-EM cluster**

Step 5 A message appears with the following options:

- **[cancel]—**Exit the configuration wizard.
- **[proceed]—**Begin the process to remove this host from its cluster.

Choose **proceed>>** to begin. After choosing **proceed>>**, the configuration wizard begins to remove this host from its cluster.
At the end of this process, this host is removed from the cluster.

Step 6 Repeat the above steps (steps 1-5) on a second host in the cluster.

Note You must repeat the above steps on each host in your cluster, until you only have a single host remaining. You must make your configuration changes on this final remaining host.

Step 7 Using a Secure Shell (SSH) client, log into that final host in your cluster and run the configuration wizard.

```
$ config_wizard
```

After logging into the host, begin the configuration process.

Step 8 Make any necessary changes to the configuration values for the external network settings, NTP server address, and/or password for the Linux grapevine user using the wizard.
After making your configuration change(s), continue through the configuration process to the final message.

Step 9 At the end of the configuration process, a final message appears stating that the wizard is now ready to proceed with applying the configuration.
The following options are available:

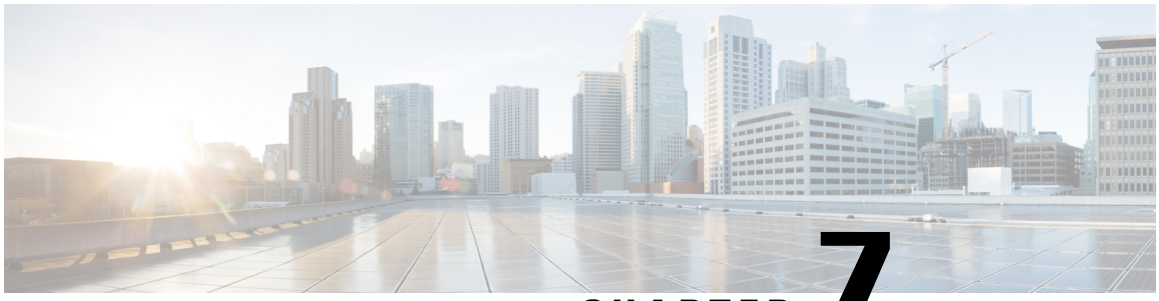
- **[back]—**Review and verify your configuration settings.
- **[cancel]—**Discard your configuration settings and exit the configuration wizard.
- **[save & exit]—**Save your configuration settings and exit the configuration wizard.
- **[proceed]—**Save your configuration settings and begin applying them.

Enter **proceed>>** to complete the installation. After entering **proceed>>**, the configuration wizard applies the configuration values that you entered above.

Note

At the end of the configuration process, a **CONFIGURATION SUCCEEDED!** message appears.

Step 10 Log into the other hosts in your multi-host cluster and use the configuration wizard to recreate the cluster.
Refer to *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide* for information about this specific procedure.



CHAPTER 7

Troubleshooting Services Using System Health

The following procedures may be used to troubleshoot services using the **System Health** tab in the Cisco APIC-EM GUI:

- About Cisco APIC-EM Services, page 51
- Reviewing the Service Version and Status Using the SYSTEM HEALTH Tab, page 53
- Removing a Service Instance Using the SYSTEM HEALTH Tab, page 55
- Creating a Service Instance Using the SYSTEM HEALTH Tab, page 56

About Cisco APIC-EM Services

The Cisco APIC-EM creates a Platform as a Service (PaaS) environment for your network, using Grapevine as an Elastic Services platform to support the controller's infrastructure and services. A service in this PaaS environment is a horizontally scalable application that adds instances of itself when demand increases, and frees instances of itself when demand decreases.

The Cisco APIC-EM controls elasticity at the service level, rather than at the Grapevine client level.

Service Managers and Monitors

The Cisco APIC-EM services that run on the Grapevine Elastic Services Platform provide the controller with its functionality. The Grapevine Elastic Services Platform consists the following components:

- Grapevine root—Handles all policy management in regards to service updates, as well as the service lifecycle for both itself and the Grapevine client.
- Grapevine client—Location where the supported services run.

After installation, service functionality is enabled using the following managers and monitors:

- Grapevine Root
  - Service manager—Starts, stops, and monitors service instances across the Grapevine clients.
  - Capacity manager—Provides on-demand capacity to run the services.

- Load monitor—Monitors the load and health of services across the Grapevine clients.
- Service catalog—Repository of service bundles that can be deployed on the Grapevine clients.

- Grapevine Client
  - Service manager—Starts, stops, and monitors service instances on the Grapevine client.
  - Service instance manager—Deploys the service.

Service Features

The Cisco APIC-EM provides the following service features:

- Adding capacity on an existing client—When a service load exceeds a specified threshold on a client, the controller can request another service instance to start on a second, preexisting client.
- Adding capacity on a newly instantiated client—When a service load exceeds a specified threshold on a client, the controller can request a new client to be instantiated and then start another service instance on this client.
- Allows automatic scaling of services—As the service load increases, the controller instantiates additional service instances in response. As the service load decreases, the controller tears down the number of instances in response.
- Resiliency for services—When a service fails, the controller starts a replacement instance. The controller then ensures that the service's minimum instance count requirements are maintained.

Services

The following is a list of default Cisco APIC-EM services for the Cisco APIC-EM Release 1.5.x.

- access-policy-programmer-service
- apic-em-event-service
- apic-em-inventory-manager-service
- apic-em-jboss-ejbca
- apic-em-network-programmer-service
- apic-em-pki-broker-service
- cas-service
- cassandra
- election-service
- file-service
- grapevine
- grapevine-coordinator-service

- grapevine-log-collector
- grouping-service
- identity-manager-pxgrid-service
- nbar-policy-programmer-service
- network-poller-service
- node-ui
- pnp-service
- policy-analysis-service
- policy-manager-service
- postgres
- qos-lan-policy-programmer-service
- qos-monitoring-service
- qos-policy-programmer-service
- rabbitmq
- rbac-service
- reverse-proxy
- router
- scheduler-service
- task-service
- telemetry-service
- topology-service

Note The Cisco APIC-EM services running on your controller is dependent upon the applications installed and enabled on the host.

Reviewing the Service Version and Status Using the SYSTEM HEALTH Tab

You are able to perform the following tasks using the **SYSTEM HEALTH** tab in the **Home** page of the Cisco APIC-EM GUI:

- Review the status of each service
- Review the number of instances of each service running
- Review the version of each service

- Review the IP address of the host where the service is running

Before You Begin

You must have successfully installed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Step 1 Log into the controller to view the controller's GUI.

Step 2 Click the **SYSTEM HEALTH** tab in the **Home** page to view information about the controller's health.
The following information is displayed in the **SYSTEM HEALTH** tab.

System (Host) Health Data	Data displayed include: • Host IP address • CPU—Host CPU usage is displayed in MHZ. Both the currently used and available host CPU is displayed. • Memory—Host memory usage is displayed in GB. Both the currently used and available host memory is displayed. • Storage—Host storage usage is displayed in GB. Both the currently used and available host storage is displayed. Color indicates status for the above host data: • Green—Indicates proper usage and support. • Yellow—Indicates usage is approaching improper levels and triggers this warning (color change). • Red—Indicates a failure based upon the usage exceeding the maximum supported value. Additionally, a graphical representation of the above data over the last 24 hours is displayed in this tab. Moving your cursor or mousing over the graph displays a data summation for specific date and time. **Note** By placing your cursor over (mouseover) a color warning in the window, further information about the warning or failure message appears.

Application Health Data	Displays applications available from the **Navigation** pane, and the services that support each application. For example, the **Topology** application accessible in the GUI is supported by topology-service. Color bars indicate the status for the applications and the supporting service(s): • Green —Indicates that an application instance is starting. An application instance is the aggregation of the service instances. You can configure a minimum or maximum number of service instances, as well as grow and harvest these service instances (spin up or spin down the services). • Yellow—Indicates application instance and its supporting service instance(s) are experiencing issues and triggers this warning (color change). • Red—Indicates a failure of the application instance and its supporting service instance(s). You can harvest a service instance and then regrow it using the GUI. If the service instance does not regrow using the GUI, then you can manually regrow it. When you harvest a service instance, the controller will determine which instance is regrown (load balancing among them). • Blue—Indicates an in-progress state for the application or service instance (growing or harvesting).

Step 3 Review the status and version of each service and application listed in the **SYSTEM HEALTH** tab.

What to Do Next

If there are any problems with any of the services or applications, then review the following procedures to troubleshoot a service.

Removing a Service Instance Using the SYSTEM HEALTH Tab

You are able to remove or harvest a service instance manually by using the **SYSTEM HEALTH** tab in the controller's GUI. You may wish to harvest a service instance and then regrow (recreate) it to correct for a faulty or unstable service.

Caution Only advanced users should perform the tasks described in this procedure or attempt to troubleshoot the services.

Before You Begin

You must have successfully installed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Step 1 Log into the controller to view the controller's GUI.

Step 2 Click the **SYSTEM HEALTH** tab in the **Home** page to view information about the controller's health.
For information about what is displayed in the **SYSTEM HEALTH** tab, see Reviewing the Service Version and Status Using the SYSTEM HEALTH Tab, on page 53.

Step 3 Review the list of *operational* services in the **SYSTEM HEALTH** tab.
Each service is represented by a square. A green-tinged colored square represents an active instance of the service, and a red-tinged colored square represents a service with a faulty or failed instance. Squares without color represents inactive services (no instances initiated and running).

Note Placing your cursor over a square displays the version of the service, number of instances running, and host IP address where the service instance is running.

Step 4 Locate the service where you want to manually remove (harvest) an instance of a service and click the subtraction sign (-) at the upper right.
You are then prompted to confirm your action to remove a service instance.

Step 5 Choose **Yes** in the dialog box to confirm that you want to remove an instance of the service.
The instance of the service is then spun down.

When the process is finished, the square representing the service instance is removed.

What to Do Next

Manage your services by either manually removing (harvesting) additional instances or growing (restoring) instances for the services.

Creating a Service Instance Using the SYSTEM HEALTH Tab

You are able to create or restore a service instance manually by using the **SYSTEM HEALTH** tab in the controller's GUI. You may wish to create or restore a service after previously harvesting or removing it for faulty or unstable behavior.

Caution Only advanced users should perform the tasks described in this procedure or attempt to troubleshoot the services.

Before You Begin

You must have successfully installed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Step 1 Log into the controller to view the controller's GUI.

Step 2 Click the **SYSTEM HEALTH** tab in the **Home** page to view information about the controller's health.
For information about what is displayed in the **SYSTEM HEALTH** tab, see Reviewing the Service Version and Status Using the SYSTEM HEALTH Tab

Step 3 Review the list of *operational* services in the **SYSTEM HEALTH** tab.
Each service is represented by a square. A green-tinged colored square represents an active instance of the service, and a red-tinged colored square represents a service with a faulty or failed instance. Squares without color represents inactive services (no instances initiated and running).

Note Placing your cursor over a square displays the version of the service, number of instances running, and host IP address where the service instance is running.

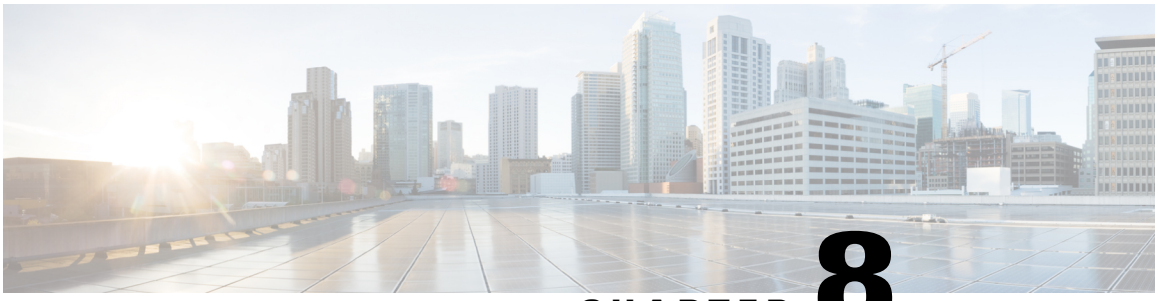
Step 4 Locate the service where you want to manually create or restore an instance of a service and click the addition sign (+) at the upper right.
You are then prompted to confirm your action to create or restore an instance.

Step 5 Choose **Yes** in the dialog box to confirm that you want to create or restore an instance of the service.
The instance of the service is then spun up.

When the process is finished, the square representing the service instance is created.

What to Do Next

Manage your services by manually growing (restoring) additional instances or removing (harvesting) instances from the services.



CHAPTER 8

Troubleshooting Services Using the Controller Admin Console

The following procedures may be used to troubleshoot services using the controller admin console:

- About Cisco APIC-EM Services, page 59
- Controller Admin Console, page 61
- Reviewing the Service's Version, Status, and Logs, page 62
- Removing a Service Instance, page 64
- Creating a Service Instance, page 66

About Cisco APIC-EM Services

The Cisco APIC-EM creates a Platform as a Service (PaaS) environment for your network, using Grapevine as an Elastic Services platform to support the controller's infrastructure and services. A service in this PaaS environment is a horizontally scalable application that adds instances of itself when demand increases, and frees instances of itself when demand decreases.

The Cisco APIC-EM controls elasticity at the service level, rather than at the Grapevine client level.

Service Managers and Monitors

The Cisco APIC-EM services that run on the Grapevine Elastic Services Platform provide the controller with its functionality. The Grapevine Elastic Services Platform consists the following components:

- Grapevine root—Handles all policy management in regards to service updates, as well as the service lifecycle for both itself and the Grapevine client.
- Grapevine client—Location where the supported services run.

After installation, service functionality is enabled using the following managers and monitors:

- Grapevine Root

- Service manager—Starts, stops, and monitors service instances across the Grapevine clients.
- Capacity manager—Provides on-demand capacity to run the services.
- Load monitor—Monitors the load and health of services across the Grapevine clients.
- Service catalog—Repository of service bundles that can be deployed on the Grapevine clients.

- Grapevine Client
  - Service manager—Starts, stops, and monitors service instances on the Grapevine client.
  - Service instance manager—Deploys the service.

Service Features

The Cisco APIC-EM provides the following service features:

- Adding capacity on an existing client—When a service load exceeds a specified threshold on a client, the controller can request another service instance to start on a second, preexisting client.
- Adding capacity on a newly instantiated client—When a service load exceeds a specified threshold on a client, the controller can request a new client to be instantiated and then start another service instance on this client.
- Allows automatic scaling of services—As the service load increases, the controller instantiates additional service instances in response. As the service load decreases, the controller tears down the number of instances in response.
- Resiliency for services—When a service fails, the controller starts a replacement instance. The controller then ensures that the service's minimum instance count requirements are maintained.

Services

The following is a list of default Cisco APIC-EM services for the Cisco APIC-EM Release 1.5.x.

- access-policy-programmer-service
- apic-em-event-service
- apic-em-inventory-manager-service
- apic-em-jboss-ejbca
- apic-em-network-programmer-service
- apic-em-pki-broker-service
- cas-service
- cassandra
- election-service
- file-service

- grapevine
- grapevine-coordinator-service
- grapevine-log-collector
- grouping-service
- identity-manager-pxgrid-service
- nbar-policy-programmer-service
- network-poller-service
- node-ui
- pnp-service
- policy-analysis-service
- policy-manager-service
- postgres
- qos-lan-policy-programmer-service
- qos-monitoring-service
- qos-policy-programmer-service
- rabbitmq
- rbac-service
- reverse-proxy
- router
- scheduler-service
- task-service
- telemetry-service
- topology-service

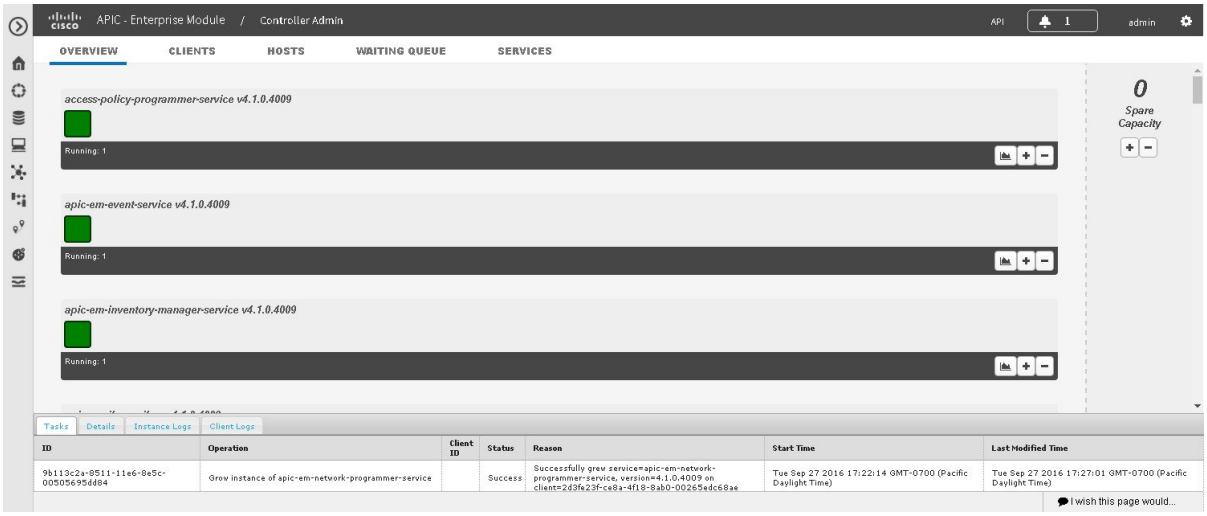
Note The Cisco APIC-EM services running on your controller is dependent upon the applications installed and enabled on the host.

Controller Admin Console

The Cisco APIC-EM creates a Platform as a Service (PaaS) environment for your network. A service in this PaaS environment is a horizontally scalable application that adds instances of itself when increasing loads occur on a client within the network. You use the **Controller Admin** console to manage and troubleshoot

these services. The **Controller Admin** console and its tools were bundled with the deployment files and installed when you first deployed the Cisco APIC-EM.

Figure 1: Controller Admin Console



Note For a multi-host cluster, you do not have to log into each host to view the **Controller Admin** console. In a multi-host cluster, you get a single, consolidated view of all of the services running on all three hosts.

The **Controller Admin** console is directly accessible from the controller's GUI. To access this console, click on **Settings** (gear) icon in the menu bar at the top of the controller's GUI, then click on the **System Administration** link in the drop down menu.

The **Controller Admin** console provides the following windows and functionality:

- **Overview—**Provides a list of services with information about their version and status. You can add or remove services in this window.
- **Clients—**Provides detailed client information in this window.
- **Hosts—**Provides detailed host information in this window.
- **Waiting Queue—**Provides information about the waiting queue.
- **Services—**Provides detailed service information. You can add or remove services in this window.
- **Logs—**Provides detailed task, instance, and client logs.

Reviewing the Service's Version, Status, and Logs

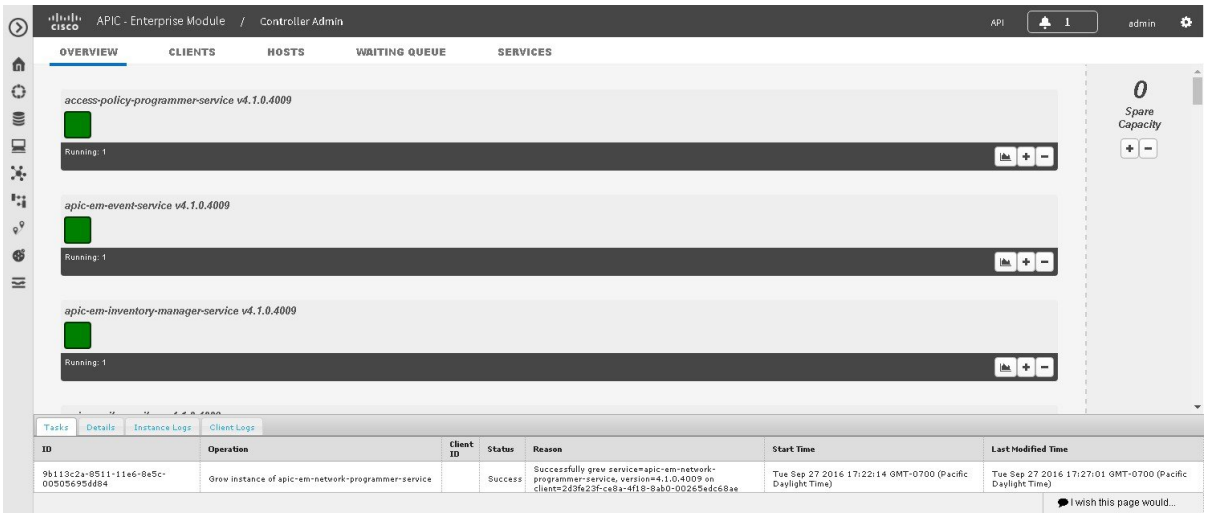
You are able to perform the following tasks using the **Controller Admin** console:

- Review the status of each service
- Review the version of each service

- Review the logs of each service

Caution Only advanced users should access the **Controller Admin** console to perform the tasks described in this procedure or attempt to troubleshoot the services.

Figure 2: Controller Admin Console



Before You Begin

You must have successfully installed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **System Administration** link from the drop-down menu.

Step 3 Review the status of each service listed in the **Overview** window in the console.
Each service is represented by a square. A green colored square represents an active instance of the service, and a red colored square represents a service with a faulty or failed instance. Squares without color represents inactive services (no instances initiated and running).

In a multi-host environment, a service may be represented by two green colored squares, indicating that the service is running on two different hosts within your cluster. Place your cursor over each square to view the host (IP address) that the service is running on.

Step 4 Review the version of each service in the **Overview** window in the console.
The version is located in the header of each listed service.

Step 5 Review the service logs by clicking a specific active instance of a service (green square icon) and then viewing the **Instance** or **Client** logs located at the bottom of the window.
The **Instance** logs detail information about the instance of the service. The **Client** logs detail information about the client where the service is located.

Step 6 Proceed to review the logs under the **Tasks** tab. The following information is available for the service task:

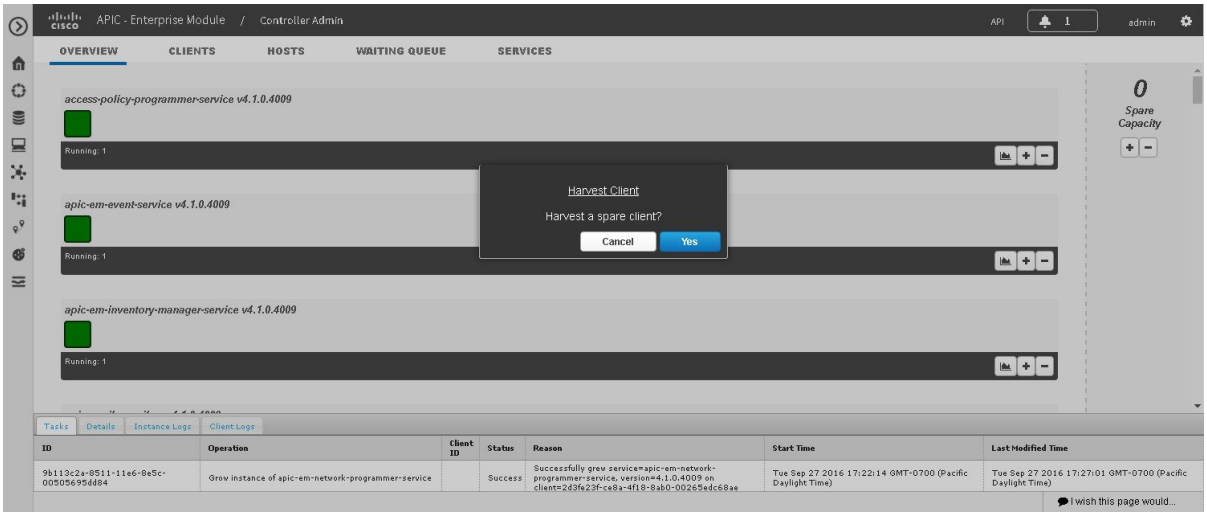
ID	Task identification number
Operation	Type of task, for example, growing a service
Client ID	Client identification number
Status	Status of the task, for example **Success** or **Failed**.
Reason	Reason given for either a successful or failed task.
Start Time	Time task stared.
Last Modified Time	Time service was last modified.

Removing a Service Instance

You are able to remove or harvest a service instance by using the **Controller Admin** console. The **Controller Admin** console tools are bundled within the ISO image and installed when you first deploy the Cisco APIC-EM.

Caution Only advanced users should access the **Controller Admin** console to perform the tasks described in this procedure or attempt to troubleshoot the services.

Figure 3: Removing (Harvesting) a Service Instance



Before You Begin

You must have successfully installed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **System Administration** link from the drop-down menu.

Step 3 Review the list of operational services in the **Overview** window in the console.
Each service is represented by a square. A green colored square represents an active instance of the service, and a red colored square represents a service with a faulty or failed instance. Squares without color represents inactive services (no instances initiated and running).

Placing your cursor over a square displays the IP address of the client where the service is running.

In a multi-host environment, a service may be represented by two green colored squares, indicating that the service is running on two different hosts within your cluster. Place your cursor over each square to view the host that the service is running on.

Note At the right of the console window are spare clients that are not running any service instances.

Step 4 Locate the service where you want to remove (harvest) an instance of a service and click the subtraction sign (-) at the lower right.
You are then prompted to confirm your action to harvest an instance.

Step 5 Choose **Yes** in the dialog box to confirm that you want to harvest an instance of the service. The controller then proceeds to spin down the instance of the service.

When the process is finished, the square representing the service instance is removed.

What to Do Next

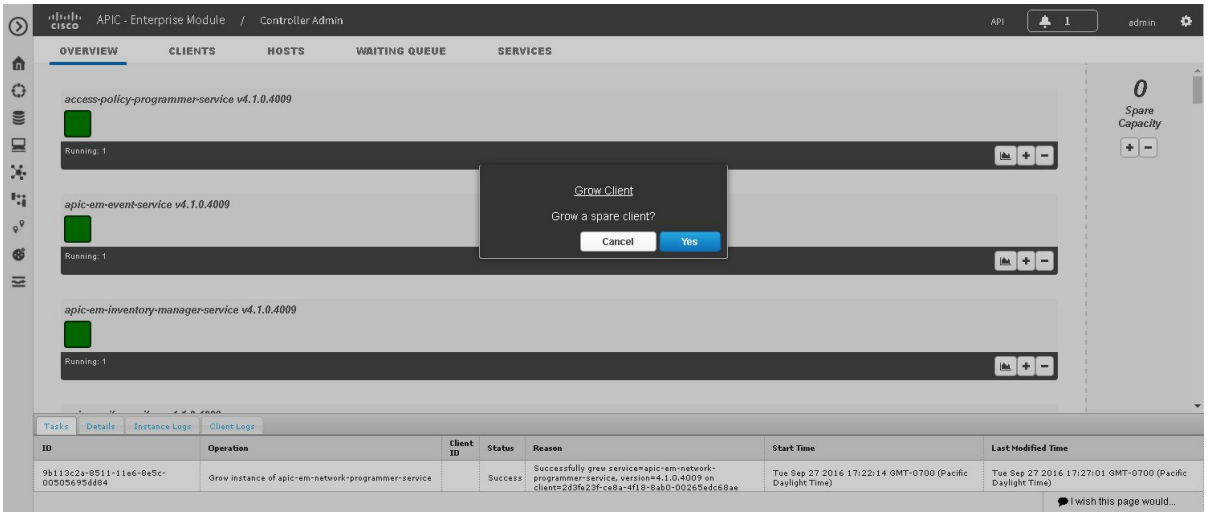
Manage your services by growing additional instances or removing (harvesting) instances from the services. When finished with the **Controller Admin** console, click another icon on the **Navigation** pane to exit the console.

Creating a Service Instance

You can create or grow a service instance using the **Controller Admin** console.

Caution Only advanced users should access the **Controller Admin** console to perform the tasks described in this procedure or attempt to troubleshoot the services.

Figure 4: Creating (Growing) a Service Instance



Before You Begin

You must have successfully installed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create

a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **System Administration** link from the drop-down menu.

Step 3 Review the list of operational services in the **Overview** window in the **Controller Admin** console.
Each service is represented by a square. A green colored square represents an active instance of the service, and a red colored square represents a service with a faulty or failed instance. Squares without color represents inactive services (no instances initiated and running).

Placing your cursor over a square displays the IP address of the client where the service is running.

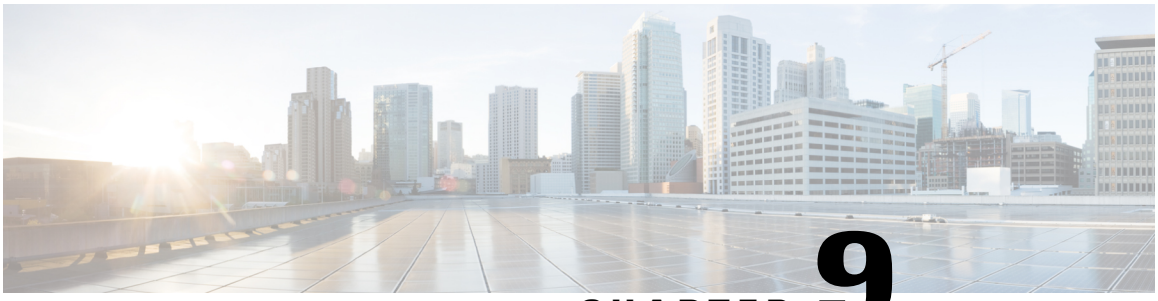
In a multi-host environment, a service may be represented by two green colored squares, indicating that the service is running on two different hosts within your cluster. Place your cursor over each square to view the host that the service is running on.

Note At the right of the console window are spare clients that are not running any service instances.

Step 4 Locate the service where you want to manually grow an instance of a service and click the addition sign (+) at the lower right.
You are then prompted to confirm your action to grow an instance.

Step 5 Choose **Yes** in the dialog box to confirm that you want to grow an instance of the service.
The controller then takes a client from the **Spare Capacity Pool** and spins up an instance of the service.

When the process is finished, the square that represents the new service instance turns green.



CHAPTER 9

Troubleshooting Using the Logs

The following logs may be used to troubleshoot Cisco APIC-EM:

- Audit Logs—Logs used primarily to monitor Cisco APIC-EM policy creation and application.
- Service Logs—Logs used to monitor Cisco APIC-EM services.

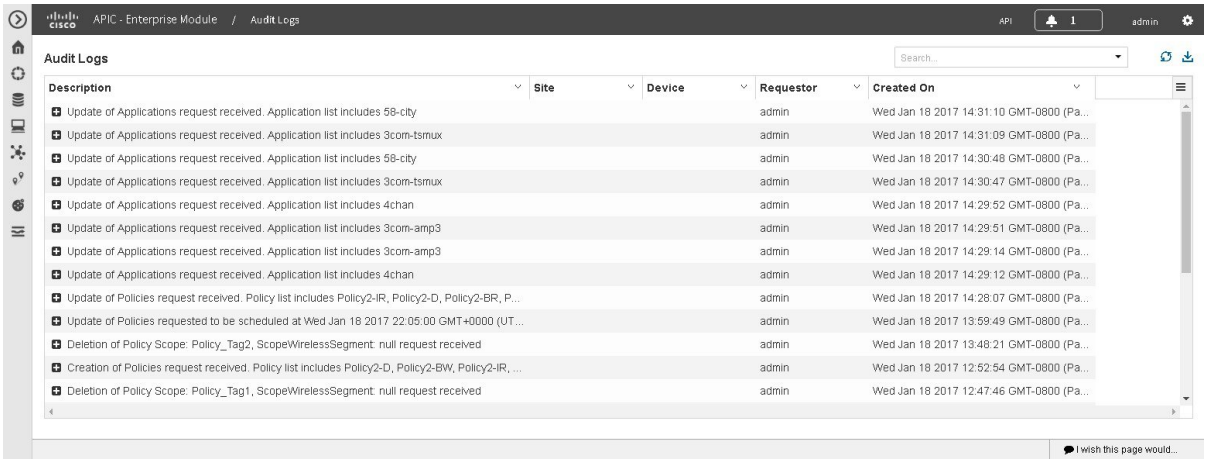
- Viewing Audit Logs, page 69
- Changing the Logging Level, page 71

Viewing Audit Logs

Audit logs capture information about the various applications (EasyQoS, PnP and IWAN). Additionally, the audit logs also capture information about device PKI notifications. The information in these audit logs can be used to assist in troubleshooting any issues involving the applications or device PKI certificates.

You can view audit logs using the **Audit Logs** window in the Cisco APIC-EM GUI. The Cisco APIC-EM also supports the ability to export the audit logs to a local system.

Figure 5: Audit Logs Window



Before You Begin

You must have successfully installed the Cisco APIC-EM and it must be operational.

You must have either administrator (ROLE_ADMIN), policy administrator (ROLE_POLICY_ADMIN), or Observer (ROLE_OBSERVER) permissions and the appropriate resource scope to perform this procedure.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Audit Logs** link from the drop-down menu.
The **Audit Logs** window appears. In the **Audit Logs** window, you can view logs about the current policies in your network. These policies were applied to network devices by either the IWAN or EasyQoS applications.

The following information is displayed for each policy in the window:

- **Description—**Application or policy audit log description
- **Site—**Name of site for the specific audit log
- **Device—**Device or devices for the audit log
- **Requestor—**User requesting audit log
- **Created On—**Date application or policy audit log was created.

Step 3 Click on the addition icon (+) next to an audit log to view the children audit logs in the **Audit Logs** window.
Each audit log can be a parent to several child audit logs. By clicking on this icon, you can view a series of additional children audit logs.

Note An audit log captures data about a task performed by the controller. Children audit logs are sub-tasks to that one task performed by the controller.

Step 4 Perform a search of the audit logs by clicking on the **Search** field in the **Audit Logs** window, entering a specific parameter, and then clicking the **Submit** button.
You can search for a specific audit log by the following parameters:

- Description
- Requestor
- Device
- Site
- Start Date
- End Date

Step 5 Click on the dual arrow icon to refresh the data displayed in the window.
The data displayed in the window is refreshed with the latest audit log data.

Step 6 Click on the down arrow icon to download a local copy of the audit log in .csv file format.
A .csv file containing audit log data is downloaded locally to your system. You can use the .csv file for additional review of the audit log or archive it as a record of activity on the controller.

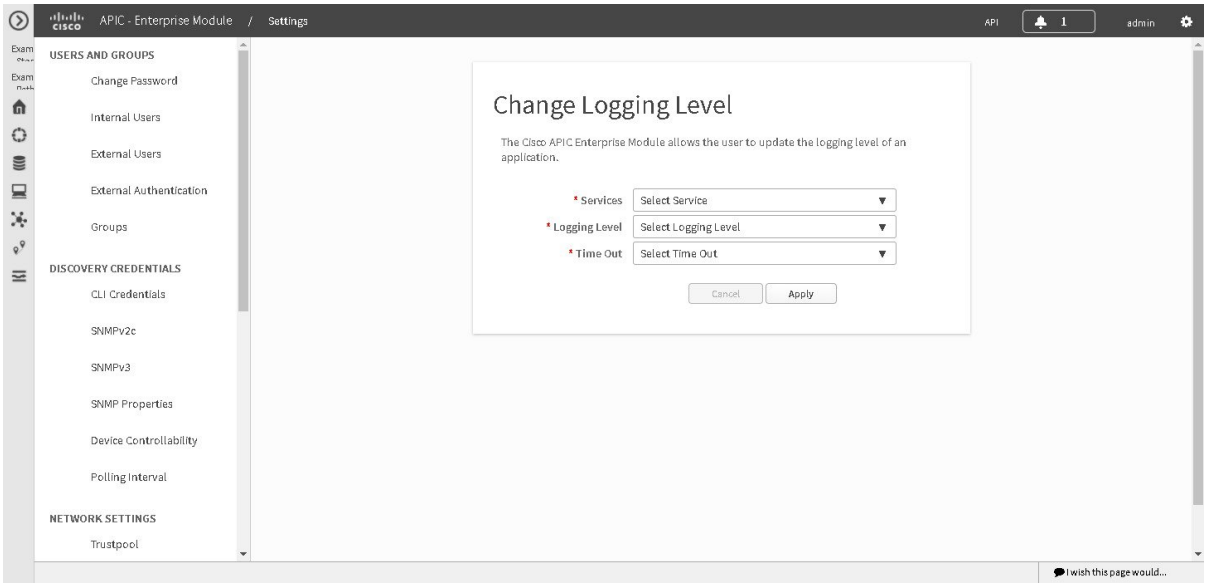
What to Do Next

Proceed to review any additional log files using the controller's GUI, or download individual audit logs as .csv files for further review or archiving purposes.

Changing the Logging Level

To assist in troubleshooting any service issues, you can change the logging level for Cisco APIC-EM services by using the **Changing the Logging Level** window in the Cisco APIC-EM GUI.

Figure 6: Service Logging Level Window



A logging level determines the amount of data that is captured to the controller's log files. Each logging level is cumulative, that is, each level contains all the data generated by the specified level and any higher levels. For example, setting the logging level to **Info** also captures **Warn** and **Error** logs. You may want to adjust the logging level to assist in troubleshooting any issues by capturing more data. For example, by adjusting the logging level you can capture more data to review in a root cause analysis or rca support file.

The default logging level for services in the controller is informational (**Info**). You can change the logging level from informational (**Info**) to a different logging level (**Debug** or **Trace**) to capture more information.

Caution Due to the type of information that may be disclosed, any logs collected at the **Debug** level or higher should be handled with restricted access.

Note The log files are created and stored in a centralized location on your controller. From this location, the controller can query and display them in the GUI. The total compressed size of the log files is 2GB. If log files created are in excess of 2GB, then the pre-existing log files are overwritten with the newer log files.

Before You Begin

You must have successfully installed the Cisco APIC-EM and it must be operational.

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Changing the Logging Level** to view the **Changing Logging Level** window. The **Logging Level** table appears with the following fields:

- **Services**
- **Logging Level**
- **Timeout**

Step 4 In the **Changing Logging Level** window, choose a service from the **Services** field to adjust its logging level.

Note The **Services** field displays any services that are currently configured and running on the controller.

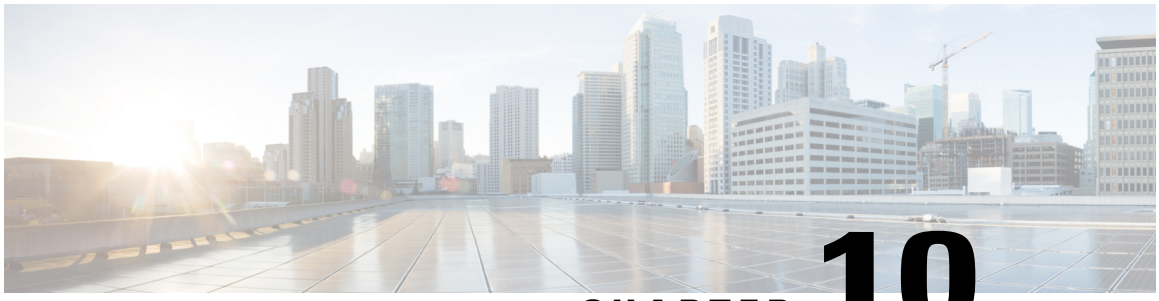
Step 5 In the **Changing Logging Level** window, choose the new logging level for the service from the **Logging Level** field. The following logging levels are supported on the controller:

- **Trace—**Trace messages
- **Debug—**Debugging messages
- **Info—**Normal but significant condition messages
- **Warn—**Warning condition messages
- **Error—**Error condition messages

Step 6 In the **Changing Logging Level** window, choose the time period for the logging level from the **Timeout** field for the logging level adjustment.
You configure logging level time periods in increments of 15 minutes up to an unlimited time period.

Step 7 Review your selection and click the **Apply** button.
To cancel your selection click the **Cancel** button.

The logging level for the specified service is set.



CHAPTER 10

Troubleshooting Passwords

The following procedures may be used to troubleshoot password problems:

- Performing Password Recovery with an Existing Administrator, page 73
- Performing Password Recovery with No Existing Administrator, page 73
- Performing Password Recovery for the Linux Grapevine User Account, page 74

Performing Password Recovery with an Existing Administrator

To perform password recovery for a user (administrator, installer or observer) where there exists at least one controller administrator (ROLE_ADMIN) user account, take the following steps:

1 Contact the existing administrator to set up a temporary password for the user that requires password recovery.

Note The administrator can set up a temporary password by deleting the user's account and then recreating it with the lost password. The user can then log back into the controller to regain access and change the password once again to whatever he or she desires.

2 The user then needs to log into the controller with the temporary password and change the password.

Note Passwords are changed in the controller GUI using the **Change Password** window. For information about changing passwords, see Managing Users and Roles in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Performing Password Recovery with No Existing Administrator

The following procedure describes how to perform password recovery where there exists only one controller administrator (ROLE_ADMIN) user account and this account cannot be successfully logged into.

Note We recommend that you create at least two administrator accounts for your deployment. With two administrator accounts, if one account is locked for whatever reason then the other account can be used to unlock that locked account.

Step 1 If there are no other existing administrator (ROLE_ADMIN) user accounts, use an SSH client from your terminal to log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 Enter the Linux username ('grapevine') and password when prompted.

Step 3 On the console, enter the following command on the Grapevine root.

```
$ config_wizard
```

This command starts up the Cisco APIC-EM configuration process.

Note The **config_wizard** command is in the PATH of the 'grapevine' user, and not the "root" user. Either run the command as the "grapevine" user, or fully qualify the command as the "root" user. For example: **/home/grapevine/bin/config_wizard**

Step 4 Choose the **<Create a new APIC-EM cluster>** option.

Step 5 Proceed through the configuration process until reaching the step to configure the **APIC-EM ADMIN USER SETTINGS**.

Step 6 Specify a new administrator user password.

Step 7 Reenter the new administrator user password for confirmation.

Step 8 Proceed through the configuration wizard and its process until completion.

Caution To save the data in the Cisco APIC-EM database as part of the reset, ensure that **no** is chosen when prompted in **HARVEST ALL VIRTUAL DISKS**.

This final step will bring down the cluster and then bring it back up again (similar to running the **reset_grapvine** command).

Performing Password Recovery for the Linux Grapevine User Account

You can use the following procedure to recover from the loss of the Linux grapevine user password. This procedure reconfigures the Linux grapevine user password that is required for accessing the host's Linux operating system.

Before You Begin

You should be logged into the host (physical or virtual) using a Linux console to access the Linux kernel.

Step 1 Reboot the host (physical or virtual) while logged into the Linux console.

Step 2 Press "e" upon seeing the GNU GRUB menu to edit the boot commands.

Note In a VMware environment, you may need to press a different key to view the GNU GRUB menu. Refer to your VMware documentation for information about access to the GNU GRUB menu. Additionally, there may be different keys to press to enter the boot sequence depending upon the BIOS used for the host.

Step 3 Search for the line in the GNU GRUB menu output that begins with "linux" and change “ro” to “rw”, and append "init=/bin/bash" to that line.
For example, search for this line:

```
linux /vmlinuz-3.13.0-24-generic root=/dev/mapper/grapevine--vg-root ro cgroup_enable=memory
swapaccount=1 quiet sqlash $vt_handoff
```

And change it to this line:

```
linux /vmlinuz-3.13.0-24-generic root=/dev/mapper/grapevine--vg-root rw cgroup_enable=memory
swapaccount=1 quiet sqlash $vt_handoff init=/bin/bash
```

Step 4 Press **Ctrl-x** or the **F10** key to proceed with the boot process.

Note We recommend that you use the **F10** key to proceed with the boot process.

At this point, the host will boot up in root mode. You can now enter the Linux **passwd** command to reset the password for the Linux grapevine user.

Step 5 Enter the Linux **passwd** command to reset the password for the Linux grapevine user.

```
$ passwd grapevine
```

Caution This procedure permits you to change the Linux **grapevine** user password. Do not change the Linux **root** user password at any point in this procedure. Resetting the Linux root user password reduces the security of the host.

Step 6 When prompted, enter a new Linux grapevine password.

Step 7 When prompted, confirm the new Linux grapevine password by entering it a second time.

Step 8 Enter the following **reboot** command to reboot the system.

```
$ /sbin/reboot -f
```

The system reboots and will start up with new configuration and password.

At the end of the reboot process, you are presented with the GNU GRUB menu.

Step 9 Press **Enter** to boot up in the Ubuntu OS.

Step 10 After booting up in the Ubuntu OS, log back into the host by entering your Linux grapevine username and password.

Note Enter the Linux grapevine password created in step 6 above.

Step 11 Restart the configuration wizard using the following command.

```
$ config_wizard
```

Proceed through the configuration wizard process by clicking **next>>** and accepting the pre-configured values until you reach the **LINUX USER SETTINGS** step.

Note The **config_wizard** command is in the PATH of the 'grapevine' user, and not the "root" user. Either run the command as the "grapevine" user, or fully qualify the command as the "root" user. For example: **/home/grapevine/bin/config_wizard**

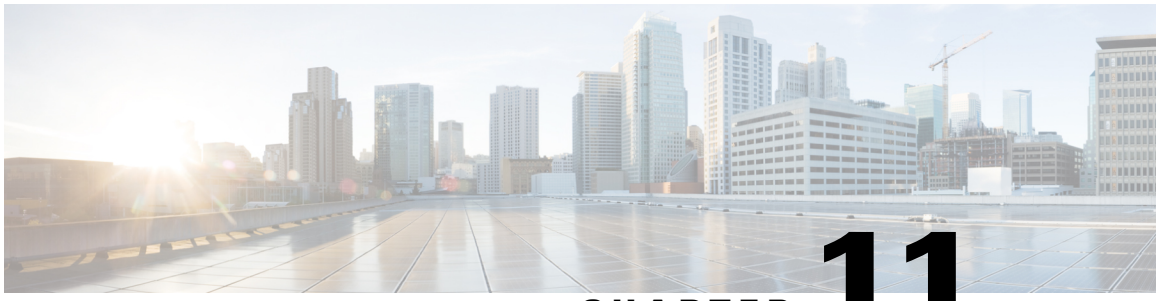
Step 12 When prompted to enter values for the **LINUX USER SETTINGS**, enter the new Linux grapevine password that you created earlier in step 6.

Note You need to start up the configuration wizard and run through the configuration process to synchronize the Linux grapevine user password to the controller itself.

Step 13 Click **next>>** and continue through the configuration wizard process, until the last step of this process.

Note When prompted to enter values for the **CONTROLLER CLEAN-UP** step, be sure to enter **no** for both **Harvest All Virtual Disks** and **Delete All Users**.

Step 14 At the end of the configuration wizard process, click **proceed>>** to have the configuration wizard save and apply your configuration changes to the Cisco APIC-EM.



CHAPTER 11

Troubleshooting Commands

The following commands are available to troubleshoot the Cisco APIC-EM:

- Root Commands, page 77
- Client Commands, page 81

Root Commands

The following tables in this section describe the commands that you can issue on the Grapevine root to troubleshoot the Cisco APIC-EM.

Note Enter the **grape help** command on Grapevine root to view a list of available commands. For more details on a specific command, type **grape help** *command_from_list*. For example, by entering **grape help update** , a new list of commands including *history* and *upload* appears. By further entering **grape help update upload**, specific command information and usage are then displayed.

The following table displays the read-only Grapevine root commands. Use these commands to display controller status, network configurations, service versions, and other key Cisco APIC-EM data to assist in troubleshooting procedures.

Table 5: Root Commands—Read Only

Command	Description
grape client display [*client_id*]	Displays the number of Grapevine clients that are currently running. This command also displays any clients that have faulted.
grape client status [*client_id*]	Displays the status of the Grapevine clients.
grapectl status	Displays the running services, their process identifiers (PID number), and uptime.

Command	Description
grape host status [*host_id*]	Displays all of the services on the host where it is issued.
grape instance display [*service_type version*]	Displays the Cisco APIC-EM services that are currently running.
grape instance status [*service_type version*]	Displays the status of the Cisco APIC-EM services.
grape network display	Displays the current external network configuration used by both Grapevine and the Cisco APIC-EM including: • IP addresses • Netmask • DNS servers
grape release display current	Displays the versions of the Cisco APIC-EM services that are currently running.
grape release display latest	Displays the latest available versions of the Cisco APIC-EM services.
grape root display [*root_id*]	Displays the Grapevine root properties, including: • hostname • interfaces • root ID • version
grape service display [*service_type* [*version*]]	Displays the Cisco APIC-EM services that are currently installed.
grape update history	Displays the Cisco APIC-EM update history and release version.
grape update_service display	Displays the current automatic services update configuration. Additional fields in the command output indicate the last time the Cisco cloud was polled for updates (`last_connect_time`), as well as the Cisco cloud status(`last_connect_status`). For example, whether the Cisco cloud is reachable, unreachable, etc.

Command	Description
grape version	Displays the version of Grapevine that the Grapevine root is running.
sudo service grapevine status	Determines the status of the Grapevine root core services and whether all of the root core services are running. You will be prompted to enter your Grapevine password for this command.

The following table displays the read and write Grapevine root commands. Use these commands to perform delete, harvest, update, and capture actions on the controller.

Caution You should exercise caution when issuing any of the read/write commands in this table.

Table 6: Root Commands-Read and Write

Command	Description
grape application disable *application_name version*	The **grape application disable** command disables an application installed on the Cisco APIC-EM. **Note** The controller's GUI also provides the user with the ability to display, disable, or enable applications, as well as providing application definitions, versions, services provided, and other important information. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide* for information about this controller GUI feature. We recommend that you use the controller's GUI when working with the applications.
grape application display *application_name version*	The **grape application display** command displays applications currently installed on the Cisco APIC-EM. This command also displays detailed information about each application's properties and their values.
grape application enable *application_name version*	The **grape application enable** command enables an application that has been uploaded to the Cisco APIC-EM.
grape application remove *application_name version*	The **grape application remove** command removes an application.

Command	Description
grape application status *application_name version*	The **grape application status** command displays the status (enabled or disabled) of applications that have been uploaded onto the Cisco APIC-EM. This command also displays the time when enabled.
grape application upload *application_bundle*	The **grape application upload** command uploads an application bundle to the Cisco APIC-EM. After an upload, you can then enable the application using the **grape application enable** command.
grape backup delete	Deletes the existing controller backup file. **Note** If you are unable to back up your current controller database, then you may want to delete it and restore an earlier smaller controller backup file.
grape host evacuate *host_id*	Harvests all of the services on the host where it is issued. If you issue this command on a host in a multi-host cluster, then the services are harvested and transferred to the remaining two hosts in the cluster. If you issue this command on a host in a single-host configuration, all the services are harvested.
grape release update force	Updates a service for Cisco APIC-EM. Use this command to force a service update.
grape config update tls_minimum	Use this command to set the TLS version to use for security for the controller. For information about supported TLS versions for the controller, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.
rca	The **rca** command runs a root cause analysis script that creates a tar file that contains log files, configuration files, and the command output. After running this command and creating the tar file, you can send the file to Cisco support for assistance in resolving an issue. For examples of using this command: • Confirming that Core Services are Running, on page 18 • Confirming the Multi-Host Cluster Configuration Values, on page 47 • Creating a Support File for a Single Host , on page 29

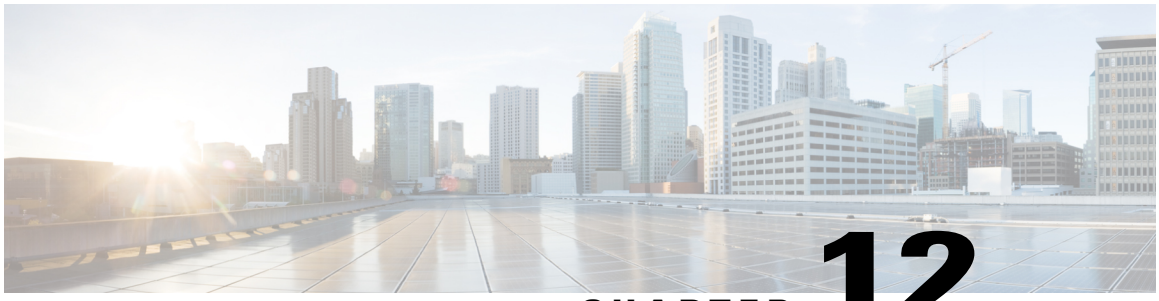
Command	Description
reset_grapevine	The **reset_grapevine** command returns the configuration settings back to values that you configured when running the configuration wizard for the first time. The configuration settings are saved to a .JSON file. This .JSON file is located at: `$ /etc/grapevine/controller-config.json`. For examples of using this command: • Resetting the Cisco APIC-EM, on page 25
reset_grapevine factory	The **reset_grapevine factory** command returns the configuration settings back to their factory defaults. **Caution** This command shuts down both Cisco APIC-EM and the host (physical or virtual) where the controller resides. After running this command, you will need to access the host and reboot it. For examples of using this command: • Restoring the Controller to the Factory Default, on page 27

Client Commands

The following table describes commands that you can issue on the Grapevine client to troubleshoot the Cisco APIC-EM.

Table 7: Client Commands- Read Only

Command	Description
grape version	Displays the version of Grapevine that the Grapevine client is running.
grapectl status	Displays the running services, their process identifiers (PID number), and uptime.



CHAPTER 12

Troubleshooting Log Files

The following log files are available to assist in troubleshooting any issues with the Cisco APIC-EM:

- Root Log Files, page 83
- Client Log Files, page 84

Root Log Files

The following table lists log files located on the Grapevine root that can be used to troubleshoot the Cisco APIC-EM.

Table 8: Root Log Files

Directory	Filename	Description
/var/log/	boot.log	This log file provides you with the details of the boot process and any errors that may occur during this process. Use this log file to troubleshoot any of the following problems: • Why did the Grapevine client fail to communicate with the Grapevine root? • Why did the Grapevine client fail to upgrade?
/var/log/	config_wizard.log	Use this log file to determine if there were any errors during the initial Grapevine configuration and deployment.

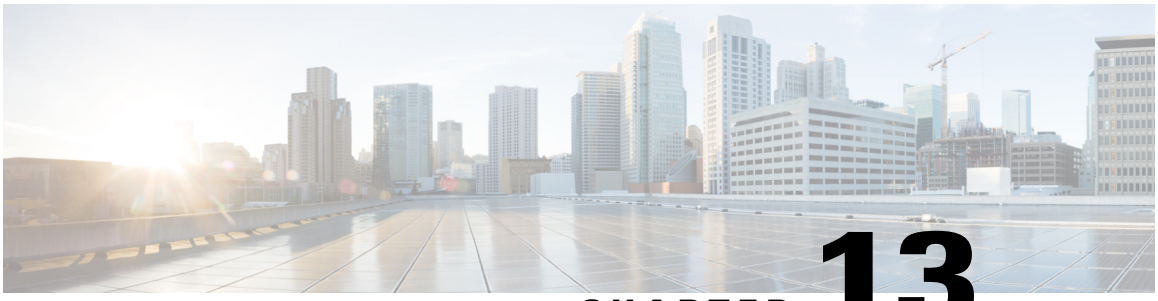
Directory	Filename	Description
/var/log/	grapevine_manager.log	Use this log file to determine if there were any errors during a manual file update using the **Update** fields in the controller's UI.
/var/log/	grapevine_manager_activity.log	Use this log file to determine if there were any errors during an update using the **Update** fields in the controller's UI.
/var/log/grapevine	supervisord.log	Use this log file to determine whether any of the Grapevine root core services unexpectedly expired.
/var/log/	cassandra.log	Use this log file to determine whether the Grapevine database is healthy.
/var/log/grapevine	grapevine_root.log	Use this log file to troubleshoot any of the following problems: • Why did Grapevine fail to grow or harvest a service instance? • Why did an automatic service update fail? • Why did Grapevine fail to communicate with a Grapevine client?
/var/log/grapevine	grapevine_capacity_manager.log	Use this log file to determine why Grapevine failed to grow or harvest a Grapevine client.
/var/log/	grapevine_application_install.log	Use this log file to view the steps performed during an application installation.

Client Log Files

The following table lists log files located on the Grapevine client that can be used to troubleshoot the Cisco APIC-EM.

Table 9: Client Log Files

Directory	Filename	Description
/var/log	boot.log	Use this log file to determine the following: • Why did this Grapevine client fail to communicate with the root? • Why did this Grapevine client fail to upgrade?
/var/log/grapevine	supervisord.log	Use this log file to determine if any of the Grapevine client core services unexpectedly died?
/var/log/grapevine	grapevine_client.log	This log file provides you with the details of the Grapevine client daemon bootstrap process and any errors that may occur during this process. Use this log file to determine the following: • Why did this Grapevine client fail to grow or harvest a service instance? • Why did this Grapevine client fail to communicate to the Grapevine root?
/var/log/grapevine/services/	[service-name]/[version]/[service-name].log	Use this log file to determine why did a service fail to perform some operation?



CHAPTER 13

Contacting the Cisco Technical Assistance Center

- Contacting the Cisco Technical Assistance Center, page 87

Contacting the Cisco Technical Assistance Center

If you cannot locate the source and potential resolution for a problem in the prior sections of this guide, then contact a Cisco customer service representative for information on how to best proceed with resolving the issue. For Cisco Technical Assistance Center (TAC), see the Cisco Information Packet publication that is shipped with your appliance or visit the following website:

http://www.cisco.com/tac/

Before you contact Cisco TAC, make sure that you have the following information ready:

- If your deployment is using a Cisco APIC-EM appliance(s), then the appliance chassis type and serial number.
- If your deployment is using a Cisco APIC-EM appliance(s), then the date you received the new Cisco APIC-EM appliance.
- The maintenance agreement or warranty information (see the Cisco Information Packet).
- The name, type of software, and version or release number (if applicable).
- A brief description of the problem or condition you experienced, the steps you have taken to isolate or re-create the problem, and a description of any steps you took to resolve the problem.

Note Be sure to provide the customer service representative with any upgrade or maintenance information that was performed on the controller after your initial installation.

Contacting the Cisco Technical Assistance Center

INDEX

A

appliances 6
audience vii
audit log 69

C

capacity manager 51, 60
Cisco APIC-EM 3
    overview 3
Cisco TAC 87
client commands 81
Controller Development console 61
core services 18
creating a support file 29

D

database 7

F

factory default 27

G

Grapevine 7

H

hosts 6

I

installation 15

L

load monitor 52, 60
log file 84
    client 84
log files 83
    root 83
logging level 71

M

multi-host 47
multi-host cluster 36, 37
multi-host cluster settings 49

N

network connections 8
    NICs 8
networks 7

P

PaaS 51, 59
password recover 73
password recovery 73, 74
    Linux user account 74

R

re-running the configuration wizard 24
related documentation ix

reset_grapevine factory command 27
resetting the Cisco APIC EM 25, 39
root 7
    client 7
root commands 77

S

SDN 51, 59
service 64
    harvest 64
service catalog 52, 60
service instance 66
    grow 66
service instance manager 52, 60
service logs 62
service manager 51, 60
service status 62
service version 62
services 7, 51, 52, 59, 60
    managers 51, 59
    monitors 51, 59
supervisor manager 52, 60
System Health 53, 55, 56
    create service 56
    remove service 55
    review service 53

T

troubleshooting 25, 39
troubleshooting matrix 9

U

update controller 19, 21
    command script 19, 21